CA Role & Compliance Manager

Portal-Benutzerhandbuch

r12.5 SP3



CA-Produktreferenzen

Dieses Dokument bezieht sich auf die folgenden Produkte von CA Technologies:

- CA Role & Compliance Manager (CA RCM)
- Identity Manager
- CA SiteMinder
- CA Enterprise Log Manager
- CA Service Desk Manager

Technischer Support – Kontaktinformationen

Wenn Sie technische Unterstützung für dieses Produkt benötigen, wenden Sie sich an den Technischen Support unter http://www.ca.com/worldwide. Dort finden Sie eine Liste mit Standorten und Telefonnummern sowie Informationen zu den Bürozeiten.

Inhalt

Kapitel 5: Verwenden von Geschäfts-Workflows 43

Kapitel 6: Ausführen von Zertifizierungskampagnen 73

Kapitel 11: Bearbeiten von Geschäftsprozessregeln 183

Kapitel 12: Verwenden von Verwaltungsfunktionen 199

Kapitel 1: Einleitung

Dieses Kapitel enthält folgende Themen:

Über dieses Handbuch

Dieses Handbuch bietet einen Überblick sowie Schritt-für-Schritt-Anweisungen zur Verwendung des CA RCM-Portals. Das CA RCM-Portal ist eine webbasierte Benutzeroberfläche, die Benutzern Zugriff auf Funktionen des Rollen- und Compliance-Managements in CA RCM bietet.

Zielgruppe

Dieses Handbuch richtet sich an Rollentechniker, Systemadministratoren und Organisationsmanager, die Berechtigungen verleihen und zertifizieren. Rollentechniker sind üblicherweise gut ausgebildete Experten, die mit der Zielorganisation vertraut sind. In diesem Handbuch wird davon ausgegangen, dass Rollentechniker entsprechend für CA RCM-Client-Tools geschult wurden und mit der CA RCM-Dokumentation vertraut sind, die dem Installationspaket des Client-Tools beiliegt.

Systemadministratoren sollten mit der CA RCM-Software vertraut sein und wissen, wie Benutzer- und Ressourcendatenbanken hoch- und runtergeladen werden sowie Kenntnisse über Rollenermittlung und Auditvorgänge besitzen. Dieses Handbuch richtet sich auch an allgemeine Administratoren und Organisationsmanager, die für zahlreiche Prozesse zuständig sind und daher im Laufe ihrer täglichen Aktivitäten auf das Portal zugreifen. Andere Benutzer haben einen eingeschränkten Zugriff auf die Optionen des CA RCM-Portals.

Kenntnisse des Microsoft-Betriebssystem und den entsprechenden Anwendungen sowie relevanter Peripherie- und Remote-Geräte werden vorausgesetzt.

Weitere Informationen:

Sicherheit und Berechtigungen (siehe Seite 285)

Häufigste Prozesse

Das CA RCM-Portal bietet Zugriff auf Informationen und Prozesse, die für eine Übersicht über systemübergreifendes Rollenmanagement, Compliance-Management, Kampagnenzertifikationen und relevantes Sicherheitsmanagement notwendig sind.

Zu den häufigen Prozessen, die Benutzer im CA RCM-Portal ausführen, zählen u. a. folgende:

Ausführen von Kampagnen

Kampagnen verwenden die Standard-Auditing-Tools von CA RCM, um Zertifikations- oder Bewertungsprozesse eines Unternehmens durch designierte Genehmiger durchzuführen. Das Ziel der Kampagne ist zu zertifizieren, dass die erteilten Berechtigungen mit den Anforderungen des Unternehmens und den festgelegten Regelungen übereinstimmen und dazu nicht in zu großem Masse zugewiesen werden. Dieser Prozess wird von der CA RCM-Auditkarteneinrichtung unterstützt, die die Darstellung von "Out-of-pattern"-liegenden und nicht der Compliance entsprechenden Informationen für den Genehmiger ermöglicht. Der Kampagnenadministrator kann Mustererkennungs-Tools und Regeln zur Richtliniendurchsetzung anwenden, um eine Konfiguration zu analysieren und ein umfassendes Audit auszuführen. Das Ergebnis eines Audits ist die Auditkarte, die alle verdächtigen Datensätze auflistet und die Art des Verdachts angibt (zurzeit etwa 50 unterschiedliche Arten).

Teil des Reinigungsprozesses und zugleich ein wichtiger Schritt vor dem Rollenkonstruktionsprozess ist für den Unternehmensmanager (Genehmiger) die Überprüfung des Zugriffsrechts. Ein Manager kann für ein Team von Benutzern, mehrere Rollen oder mehrere Ressourcen zuständig sein. In einem Unternehmen mit mehr als 1000 Benutzern wird der Reinigungsprozess mithilfe von Managern enorm beschleunigt. Je nach Definition der Kampagne muss der Unternehmensmanager möglicherweise die Zugriffsrechte der Mitarbeiter bzw. der Ressourcen, für die sie zuständig sind, überprüfen und einen Bericht der Änderungsanfragen an den CA RCM-Administrator übergeben. Kampagnen werden nicht nur in der Phase der Unternehmensreinigung verwendet, sondern auch vorschriftsmäßig für regelmäßige Zertifizierungen.

Self-Service

Manager können das CA RCM-Portal dazu verwenden, die Rollendefinitionen ihrer Teams zu verwalten und auf Unternehmensressourcen zuzugreifen. Benutzer können im Hinblick auf Systemrollen und -ressourcen ihre eigenen Berechtigungen verwalten.

Entitäten-Browser

Dieser Browser erleichtert Administratoren oder Unternehmensmanagern, die das CA RCM-Portal verwenden, die Ansicht der Entitäten (z. B. Benutzer, Rollen, Ressourcen) im Zusammenhang mit einem bestimmten Universum und in einer bestimmten Konfiguration. Die Informationen werden in einer Tabelle angezeigt. Die Tabelle enthält grundlegende Informationen für jede Entität.

Berichte ausführen

Bietet Zugriff auf eine Vielfalt von Berichten, wie Berichte, die Benutzer, Ressourcen oder Rollen und deren Verknüpfungen zu anderen Entitäten auflisten; Berichte, die den Status einer Kampagne verfolgen, und andere.

Hinweis: Weitere Informationen über die Berichte, die CA RCM unterstützt, finden Sie im Abschnitt "Berichtstypen" (siehe Seite 176).

Dashboards

Zeigt Benutzern bei der Ausführung Ihrer Aufgaben automatisch nützliche Informationen zur Statistik. CA RCM schließt die folgenden Dashboards ein:

- Konfigurations-Dashboard
- Auditkarten-Dashboard
- Compliance-Dashboard
- Rollenabdeckungs-Dashboard
- Zertifizierungs-Dashboard

Verwaltung

Administratoren können ein Universum erstellen, Import-/Exportconnectors generieren und deren Planung festlegen. Es können außerdem andere Funktionen durchgeführt werden, zu denen jedoch nur Senior-Administratoren berechtigt sind.

Weitere Informationen:

Verwenden der CA RCM-Portalbenutzeroberfläche (siehe Seite 17)

Kapitel 2: Verwenden der CA RCM-Portalbenutzeroberfläche

Die Benutzeroberfläche, Menüs und Optionen werden vollständig in diesem Kapitel beschrieben. Nicht alle Benutzer haben vollständige Administratorenberechtigungen, daher sind nicht alle Optionen für alle Benutzer verfügbar.

Dieses Kapitel enthält folgende Themen:

Öffnen des CA RCM-Portals

Sobald Sie CA RCM installieren und starten, können Sie die webbasierte Benutzeroberfläche auf einem Remote-Computer über die URL des CA RCM-Portals öffnen.

So öffnen Sie das CA RCM-Portal

1. Öffnen Sie einen Webbrowser und geben Sie *eine* der folgenden URLs ein:
   - Um keine SSL-Verbindung zu verwenden, geben Sie die folgende URL ein:

     `http://`*`ServerName`*`:`*`Port`*`/eurekify`
   - Um eine SSL-Verbindung zu verwenden, geben Sie die folgende URL ein:

     `https://`*`ServerName`*`:`*`HTTPSPort`*`/eurekify`

   Der Anmeldebildschirm wird geöffnet.
2. Geben Sie Ihre Anmeldedaten ein.

   Hinweis: Beim Kennwort muss die Groß-/Kleinschreibung beachtet werden.
3. Klicken Sie auf "Anmelden".

   Die Startseite des CA RCM-Portals wird angezeigt.

Weitere Informationen:

Verwenden der CA RCM-Portalbenutzeroberfläche (siehe Seite 17)

Benutzeroberfläche

Sie können die folgenden allgemeinen Funktionen zur Nutzbarkeit in den Fenstern des CA RCM-Portals verwenden:

- Automatische Vervollständigung – In Feldern, die sich auf Feldnamen oder Werte einer Datei beziehen, werden Ihre Angaben vom Portal mit entsprechenden Daten der Datendatei vervollständigt. Sie können auch den Pfeil nach unten verwenden, um durch eine Liste von verfügbaren Feldwerten zu blättern.
- Pflichtfelder – Felder, die mit einem orangen Punkt markiert sind, sind obligatorisch auszufüllen. Sie können nicht mit dem nächsten Schritt eines Prozesses fortfahren, ohne diese Felder auszufüllen.
- Anpassbare Tabellen – Klicken Sie in der Kopfzeile der Tabelle auf "Anpassen", um die angezeigten Spalten sowie die Reihenfolge zu verändern, in der sie angezeigt werden. Klicken Sie auf einen Spaltenkopf, um die Tabelle nach den Werten in dieser Spalte zu sortieren. Sie können auch die Dropdown-Liste "Datensätze pro Seite" verwenden, um die Größe einer langen Tabelle zu beschränken oder zu erweitern.

Benutzeroberfläche (Non-Administrators)

Verschiedene Arten von Benutzern melden sich beim CA RCM-Portal an:

- Administratoren und Rolleningenieure verwenden CA RCM, um das Datenuniversum zu formen und zu verwalten. Sie konfigurieren Datenconnectors, die das Universumsmodell aktualisieren und exportieren Änderungen in Berechtigungseinstellungen auf Bereitstellungsendpunkte. Sie definieren und führen Zertifizierungskampagnen aus, um Benutzerberechtigungen zu überprüfen.
- Unternehmensmanager interagieren mit CA RCM hauptsächlich als Teilnehmer in Zertifizierungskampagnen. Sie können auch die Funktionen des Rollenmanagements im Portal verwenden, um die Berechtigungen von Benutzern oder Ressourcen, die sie verwalten, zu ändern. All diese Aufgaben werden über ein Aufgabenverwaltungssystem abgewickelt, dessen Grundlage Tickets sind.

Wenn sich Benutzer beim CA RCM-Portal anmelden, können sie nur auf die Portalfunktionen zugreifen, die relevant für sie sind. Unternehmensmanager können nur auf ihren eigenen Posteingang, den Bereich Rollenmanagement und andere relevante Bereiche des Portals zugreifen. Administratoren können auf alle Bereiche des Portals zugreifen. Sie können Datenuniversen und Connectors definieren und Kampagnen erstellen.

Weitere Informationen:

Sicherheit und Berechtigungen (siehe Seite 285)

Unterstützte Sprachen

Die Benutzeroberfläche des CA RCM-Portals erscheint in der Sprache, die während der Installation ausgewählt wurde. Um sicherzustellen, dass Textrichtung, Datumsformate und andere Aspekte der Benutzeroberfläche mit der ausgewählten Sprache konform sind, stellen Sie die Sprache Ihres Webbrowsers auf die Sprache der Benutzeroberfläche ein.

Kapitel 3: Erste Schritte

In diesem Kapitel wird die Prozessreihenfolge beschrieben, die befolgt werden muss, wenn das CA RCM-Portal auf einem System ausgeführt wird, auf dem die Daten zu Benutzern, Rollen und Ressourcen noch nicht vom CA RCM-System heruntergeladen wurden. Die genauen Details zu den einzelnen Schritten der genannten Vorgänge werden in den folgenden Kapiteln beschrieben.

Dieses Kapitel enthält folgende Themen:

Schritt 1: Erstellen von Universen

Ein Universum ist ein virtueller Speicherort, der die gesammelten Daten der Enterprise Security- bzw. Identity Management-Systeme beinhaltet. Diese Daten werden in den CA RCM-Konfigurationsdateien gespeichert. Ein Universum besteht aus einem bestimmten Master-/Modellkonfigurationspaar. Damit wird ermöglicht, Unterschiede zwischen der "tatsächlichen", vom System (Master) importierten Konfiguration und der gewünschten Konfiguration, die nach einer Kampagne (Modell) generiert wird, zu verfolgen.

Sie brauchen die folgenden Informationen, um ein Universum zu erstellen (siehe Seite 29):

- Dateiname und Pfad der Masterkonfiguration
- Dateiname und Pfad der Modellkonfiguration
- (Optional) Genehmigte Auditkarte
- Name und Pfad der Auditeinstellungsdatei
- Namen der Felder (in den Konfigurationsdateien), die die folgenden Informationen enthalten:
  - Anmeldung
  - E-Mail
  - Benutzermanager

- Rollenmanager
- Ressourcenmanager

Hinweis: Sie können die Namen von Konfigurationsdateien angeben, die noch nicht vorhanden sind. Da Sie noch nicht über die Feldnamen verfügen, erstellen Sie die Master-/Modellkonfigurationsdateien später und aktualisieren Sie dann das Universum mit den richtigen Feldnamen.

Schritt 2: Erstellen von Importconnectors

Nachdem Sie das Universum definiert haben, für das Sie ein Audit durchführen möchten, können Sie Benutzer und Benutzerberechtigungen aus verschiedenen Endpunkten heraus importieren. Dazu müssen Sie Importconnectors definieren.

"Importieren" bedeutet hier das Herunterladen von Informationen über Benutzer, Ressourcen und Rollen von einem Endpunktsystem in CA RCM. Exportieren bedeutet hier das Hochladen von Änderungen der Informationen von Benutzern, Ressourcen und Rollen, die nach einem Audit generiert wurden.

Hinweis: Weitere Informationen zu Connectors finden Sie im Abschnitt "Verwenden von Verwaltungsfunktionen" in diesem Handbuch.

Weitere Informationen:

Import- und Exportconnectors (siehe Seite 205)

Schritt 3: Importieren von Entitätendaten

“Import” beschreibt das Herunterladen der Systemkonfigurationsdaten der aktuellen Benutzer, Ressourcen und Rollen (wenn vorhanden). Sie können den Import-Connector, den Sie im Schritt 2 erstellt haben, verwenden, um die Entitätendaten von den Unternehmensendpunkten herunterzuladen.

Sie können auch die Import-Option in der Menüleiste von CA RCM Data Management verwenden, um Entitätendaten zu importieren (mehr dazu im *Data Management-Handbuch*).

Das Ergebnis des Importprozesses ist ein Sage-Konfigurationsdokument (.cfg-Datei), das die Stufe für den Rollenermittlungsprozess festlegt.

Entitäten und Verknüpfungen: Wie CA RCM Berechtigungsinformationen anzeigt

Nachdem Sie die Konfigurationsdaten für aktuellen Benutzer, Ressource und Rolle importiert haben (soweit verfügbar), analysiert CA RCM die Bereitstellungs- und Benutzerzugriffsinformationen Ihres Unternehmens und speichert sie in Entitäten und Verknüpfungen.

Entitäten sind die Benutzer und Ressourcen in Ihrem Unternehmen. In ähnlicher Weise sind die Rollen, die CA RCM verwendet, um Zugriffsberechtigungen zu verwalten, Entitäten.

Links sind Verbindungen zwischen zwei Entitäten, durch die Zugriffsberechtigungen definiert werden. Beispiel:

- Ein Link zwischen einem Benutzer und einer Ressource erlaubt dem Benutzer den Zugriff auf diese Ressource. Sie überprüfen und genehmigen Verknüpfungen dieses Typs, wenn Sie die Berechtigungen eines Mitarbeiters zertifizieren, den Sie verwalten.
- Eine Verknüpfung zwischen einer Rolle und einer Ressource schließt die Ressource in die Rolle ein. Alle Benutzer, denen die Rolle zugewiesen wird, können auf die Ressource zugreifen.
- Eine Verknüpfung zwischen einer Rolle und einer anderen Rolle definiert über-/untergeordnete Beziehungen in der Rollenhierarchie, die CA RCM erstellt.

Zwei Entitäten können auf folgende Weisen veknüpft werden:

Direkte Links

Ein einzelner Link verbindet zwei Entitäten miteinander.

Indirekte Links

Zwei oder mehr Links verbinden die Entitäten über andere Entitäten. Wenn zum Beispiel einem Benutzer eine Rolle zugewiesen wird, die eine Ressource einschließt, werden der Benutzer und die Ressource indirekt über die Rolle miteinander verknüpft.

Duale Links

Sowohl direkte als auch indirekte Links verbinden zwei Entitäten miteinander. Zum Beispiel gewährt ein direkter Link einem Benutzer Zugriff auf eine Ressource, und es wird ihm auch eine Rolle zugewiesen, die jene Ressource einschließt.

Direkte Links und duale Links werden bei den verschiedenen Überprüfungsprozessen untersucht, zum Beispiel bei Kampagnen oder wenn einem bestimmten Geschäftsteam eine Rolle zugewiesen wird. Indirekte Links werden zur Vollständigkeit zwar aufgelistet, unterliegen jedoch nicht den Überprüfungsprozessen.

Schritt 4: Erstellen von Master-/Modellkonfigurationen

Bei der Erstellung des Universums haben Sie zwei Konfigurationsdateien angegeben: Masterkonfigurationsdatei und Modellkonfigurationsdatei. Die Masterkonfigurationsdatei enthält die Daten, die aus den Endpunktsystemen importiert wurden. Die Modellkonfigurationsdatei ist anfänglich eine Kopie dieser Daten und wird im Laufe der Rollenmodellierung und des Auditprozesses bearbeitet und aktualisiert.

Weitere Informationen zur Erstellung von Master- und Modellkonfigurationsdateien unter der Verwendung des CA RCM DNA-Moduls finden Sie im Anhang A: Duplizieren von Konfigurationen. Bearbeiten Sie wenn nötig das Universum, damit die aufgelisteten Master- und Modellkonfigurationen mit den von Ihnen erstellten Konfigurationen übereinstimmt.

Nachdem Sie ein Universum erstellt oder bearbeitet haben, geben Sie die dem Universum zugewiesenen Benutzer in die CA RCM-Berechtigungskonfiguration ein, damit die Benutzer Zugriff auf das CA RCM-Portal erhalten. Üblicherweise umfasst dieser Vorgang eine RACI-Synchronisierung, um jedem Benutzer die Berechtigungen zuzuweisen, die er im Portal benötigt.

Weitere Informationen:

RACI-Vorgänge (siehe Seite 272)

Schritt 5: Erstellen von Kampagnen

Eine Kampagne ist ein Auditprozess, dem die Prüfung von Links zwischen Benutzern, Rollen und Ressourcen zugrunde liegt. Zuständige Manager der verschiedenen Entitäten werden benachrichtigt, wenn eine Kampagne begonnen hat. Die Aufgaben, die während der Kampagne zugewiesen werden, werden dem Kampagneneigentümer bzw. den Genehmigern als Tickets vorgelegt. Die Tickets enthalten notwendige Informationen, um Aufgaben zu überprüfen, zu genehmigen oder abzulehnen.

Schritt 6: Exportieren von Entitätendaten

Die Unterschiede zwischen der originalen, "echten" Konfiguration, die von den Systemendpunkten (Master) importiert wurde, und der aktualisierten und korrigierten Konfiguration, die einen Auditprozess (Modell) durchlaufen hat, werden in die originalen Endpunkte exportiert. Somit werden die Informationen zu den Unternehmens- und Plattformbenutzern sowie Benutzerberechtigungen aktualisiert, wodurch Sie den Unternehmensrichtlinien und -Regelungen entsprechen.

Weitere Informationen:

Definieren von Exportconnectors (siehe Seite 214)

Kapitel 4: Das CA RCM-Universum

Nachdem Sie ein Universum erstellt haben, können Sie die universumsspezifischen Einstellungen bearbeiten. Um auf diese Einstellungen zuzugreifen, gehen Sie auf "Verwaltung", "Einstellungen", "Einstellungen des Universums", und klicken neben dem Universum, das Sie bearbeiten wollen, auf "Bearbeiten". Das Fenster "Universum bearbeiten" erscheint und zeigt mehrere Registerkarten an, mit denen verschiedene auf das Universum bezogene Einstellungen geändert werden können.

CA RCM-Universums-Übersicht

Ein *Universum* ist eine Einsicht in einen Verwaltungs-Namespace, der es CA-RCM-Administratoren ermöglicht, aus Identity Management-Systemen gesammelte Entitäten wie Benutzer, Rollen und Ressourcen, zu verwalten. Entitäts-Daten werden in Konfigurationsdateien gespeichert. Ein Universum besteht aus einem bestimmten Master-/Modellkonfigurationspaar. Damit wird ermöglicht, Unterschiede zwischen der "tatsächlichen", vom System (Master) importierten Konfiguration und der gewünschten generierten Konfiguration (Modell), zu verfolgen.

Jeder Connector, den Sie für den Datenimport und -export in CA RCM konfigurieren, muss mit seinem eigenen Universum assoziiert sein. Wenn Sie zum Beispiel Daten aus Identity Manager importieren wollen, werden diese Daten mittels des Connectors für Identity Manager gespeichert und in einem Universum verwaltet. Wenn Sie mit einem benutzerdefinierten ausführbaren Connector Daten aus der Ressource eines Drittanbieters in CA RCM importieren möchten, erstellen Sie ein gesondertes Universum dafür, um diese Drittanbieter-Ressourcendaten zu speichern und zu verwalten.

Connectors

Connectors werden definiert, damit Benutzer und Benutzerberechtigungen (Entitäten und die Links zwischen ihnen) von Unternehmenssystemen in CA RCM importiert und exportiert werden können.

Import-Connectors werden verwendet, um die Daten von Unternehmenssystemen zu erfassen. Sobald diese Daten in CA RCM sind, können Rollen-Manager die Daten aufgrund von Unternehmensrichtlinien oder regulative Compliance Daten ändern.

Am Ende des Änderungsprozesses vergleicht CA RCM die ursprüngliche Konfiguration mit der neuen Konfiguration und erstellt ein Abweichungsprotokoll (DIFF-Datei). Export-Connectors verschieben dann die sich ergebenden Konfigurationsänderungen ins Unternehmenssystem zurück.

Komponenten eines Universums

Ein Universum enthält miteinander zusammenhängende Konfigurationsdateien und Datendateien. Jedes Universum enthält die folgenden Konfigurationsdateien:

- Masterkonfiguration - eine Datei, die Informationen über reale Benutzer und deren Benutzerberechtigungen enthält.
- Modellkonfiguration - eine Datei, die als eine Kopie der Masterkonfiguration startet, dann aber aktualisiert wird, um Änderungen der Benutzerberechtigungen oder Rollenhierarchien zu erfassen.

  Hinweis: Alle Konfigurationsdateien in einem Universum haben eine gemeinsame Struktur. Wenn Sie ein Universum definieren, geben Sie an, welche Felder die eindeutige ID, E-Mail und anderen Daten für jeden Benutzer enthalten. Diese Felder werden zur Zertifizierung, Analyse und für Berichte in CA RCM verwendet. Alle Konfigurationsdateien im Universum müssen mit diesen Feldbezeichnungen übereinstimmen. Weitere Informationen über Konfigurationsdateien finden Sie im Anhang über CA RCM-Datendateien.
- RACI-Konfigurationen - Vier Dateien, die nach Analyse der Modellkonfiguration erstellt wurden, um die Benutzer zu bestimmen, die für jede Ressource Responsible oder Accountable sind, oder die für jede Ressource konsultiert bzw. informiert werden.
- Kontokonfigurationen - auf Master- und Modellkonfigurationen bezogene Dateien; sie setzen die an Endpunkten definierten Benutzerkonten mit den Benutzern in der Konfiguration miteinander in Beziehung.

Außerdem können Sie andere Konfigurationsdateien angeben, die Teile der Master- und Modelldaten bzw. neu importierte Daten enthalten. Andere mit einem Universum assoziierte Dateien können das Folgende einschließen:

- (Optional) Genehmigte Auditkarte - ein Datei, die Im Voraus genehmigte Geschäftsregelverletzungen definiert, die in den Zertifizierungsprozessen ignoriert werden.
- Auditeinstellungen - eine Datei, die das Auditverhalten für Universumskonfigurationsdateien bestimmt.

Erstellung eines Universums

Um von Identity Management-Systemen gesammelte Entitäten wie Benutzer, Rollen, und Ressourcen zu verwalten, erstellen Sie ein Universum.

So erstellen Sie ein Universum

1. Gehen Sie im CA RCM-Portal auf "Verwaltung", "Einstellungen", "Einstellungen des Universums".

   Die Universumsliste wird angezeigt.

2. Klicken Sie auf "Neu hinzufügen".

   Das Fenster "Neues Universum erstellen" wird angezeigt.

3. Geben Sie Werte für folgende Felder an:

   Name des Universums

   Gibt den Namen des Universums an.

   Hinweis: Sie können den Namen eines vorhandenen Universums nicht verändern.

   Name der Masterkonfiguration

   Gibt die Masterkonfiguration des Universums an.

Name der Modellkonfiguration

Gibt die Modellkonfiguration des Universums an.

Beachten Sie Folgendes:

- Master- und Modellkonfigurationen müssen für jedes Universum einmalig sein. Erstellen Sie *nicht* mehr als ein Universum mit derselben Master- oder Modellkonfiguration.
- Beispiel-Konfigurationsdateinamen: CA_IMmaster.cfg, CA_IMmodel.cfg.
- Konfigurationsdateinamen dürfen keine Schrägstriche ("/" oder "\") enthalten.
- Sie können Konfigurationsdateien angeben, die noch nicht existieren. Sie werden mit den Namen erstellt, die Sie angeben, wenn Sie zum ersten Mal Daten importieren.

(Optional) Genehmigte Auditkarte

(Optional) Definiert die Liste der im Voraus genehmigten Verletzungen (siehe Seite 34)für das Universum.

Genehmigte Warnungen sind

Gibt an, ob im Voraus genehmigte Verletzungen ignoriert werden (ausgeblendet) oder in der Auditkarte ausgegraut werden.

Anmeldefeld der Konfiguration

Gibt das Feld "Benutzeranmeldungs-ID" in den Universumskonfigurationsdateien an (in der Benutzerdatenbankdatei).

Hinweis: Wenn Sie die Feldnamen an dieser Stelle noch nicht zur Verfügung haben, werden die Master-/Modellkonfigurationsdateien dennoch während des anfänglichen Imports erstellt, und Sie können das Universum mit den richtigen Feldnamen später aktualisieren.

E-Mail-Feld der Konfiguration

Gibt das Feld "Benutzer-E-Mail-Adresse" in den Universumskonfigurationsdateien an (in der Benutzerdatenbankdatei).

Feld des Benutzermanagers der Konfiguration

Gibt das Feld "Benutzer-Manager-ID" in den Universumskonfigurationsdateien an (Benutzergenehmiger).

Feld des Rollenmanagers der Konfiguration

Gibt das Feld "Rollen-Manager-ID" in den Universumskonfigurationsdateien an (Rollengenehmiger).

Feld des Ressourcenmanagers der Konfiguration

Gibt das Feld in den Universumskonfigurationsdateien an, das die Ressourcenmanager-ID enthält (Ressourcengenehmiger).

Feld der Ressourcen-Anwendung der Konfiguration

Gibt das Feld in den Universumskonfigurationsdateien an, das die Endpunkt- oder Quellanwendung einer Ressource identifiziert.

Auditeinstellungsdatei

Diese Parameter und Einstellungen definieren die Audits und auf Mustern basierende Überprüfungen, die in der Masterkonfiguration immer ausgeführt werden, wenn diese importiert wird.

4. Klicken Sie auf "Speichern".

   Das Universum wurde erstellt und wird nun in der Liste "Universen" angezeigt.

Anpassen von Tabellen für ein Universum

Für jedes Universum können Sie das Tabellen-Layout anpassen, das der Entitäten-Browser und die Rollen-Management-Fenster verwenden, um die Konfigurationsdaten anzuzeigen.

Hinweis: Diese Tabellendefinitionen werden auch standardmäßig auf Kampagnentickets angewendet, die diesem Universum zugrunde liegen.

So passen Sie die Entitäten-Browser-Anzeigeneinstellungen an

1. Gehen Sie im CA RCM-Portal auf "Verwaltung", "Einstellungen","Einstellungen des Universums".

   Das Fenster der Universumsliste wird angezeigt.

2. Klicken Sie neben dem Universum, das Sie bearbeiten möchten, auf "Bearbeiten".

   Das Fenster "Bearbeiten" wird angezeigt:

3. Wählen Sie die Registerkarte "Entitätenbrowser – Einstellungen zur Anzeige" aus.

   Diese Registerkarte enthält drei Tabellenköpfe. Die Ansichten für Benutzer, Rollen und Ressourcen zeigen im Entitäten-Browserdas Layout einer jeden Entitätentabelle an.

4. Passen Sie das Tabellen-Layout folgendermaßen an:

    a. Klicken Sie auf dem Tabellenkopf, den Sie ändern wollen, auf "Anpassen".

       Das Dialogfeld "Anpassen" wird angezeigt.

    b. Verwenden Sie die Pfeiltasten, um Spalten hinzuzufügen oder zu entfernen, und um die Spalten anzuordnen.

    c. Wenn Sie die Spalten angepasst haben, klicken Sie auf OK.

    d. Klicken Sie auf das Sperrsymbol neben dem Spaltennamen, um die Spalte obligatorisch zu machen. Benutzer können eine obligatorische Spalte verschieben, können sie jedoch nicht entfernen.

       Hinweis: Obligatorische Spalten werden in Rot angezeigt.

5. Klicken Sie auf "OK".

   Der Entitäten-Browser zeigt Konfigurationen dieses Universums in den Tabellenformaten an, die Sie angegeben haben.

Anpassen der Einstellungen für Workflow-Anzeige

Für jedes Universum können Sie das Tabellen-Layout anpassen, das der Posteingang verwendet, um Aktionen anzuzeigen, wenn Sie eine Workflow-Aufgabe unter "Meine Aufgaben" öffnen.

Obligatorische Spalten können nicht aus Tabellenansichten entfernt werden. Roter Text und ein gesperrtes Schlosssymbol zeigen obligatorische Spalten in Benutzeranpassungsfenstern an. CA RCM benötigt standardmäßig einige hartkodierte obligatorische Spalten. Administratoren können bei Bedarf zusätzliche obligatorische Spalten definieren.

So passen Sie die Einstellungen für die Workflow-Anzeige an

1. Gehen Sie im CA RCM-Portal auf "Verwaltung", "Einstellungen","Einstellungen des Universums".

   Das Fenster der Universumsliste wird angezeigt.

2. Klicken Sie bei dem Universum, das Sie bearbeiten möchten, auf "Bearbeiten".

   Das Fenster "Bearbeiten" wird angezeigt:

3. Wählen Sie die Registerkarte mit den Einstellungen für die Workflow-Anzeige aus.

   Diese Registerkarte enthält vier Tabellenköpfe. Die Köpfe "Allgemeine Aktionen", "Benutzeraktionen", "Rollenaktionen", und "Ressourcenaktionen" zeigen die Tabellenlayouts für das Fenster "Meine Aufgaben" an.

4. Passen Sie das Tabellen-Layout folgendermaßen an:

   a. Klicken Sie auf dem Tabellenkopf, den Sie ändern wollen, auf "Anpassen".

      Das Dialogfeld "Anpassen" wird angezeigt.

   b. Verwenden Sie die Pfeiltasten, um Spalten hinzuzufügen oder zu entfernen, und um die Spalten anzuordnen.

   c. Wenn Sie die Spalten angepasst haben, klicken Sie auf OK.

   d. Klicken Sie auf das Sperrsymbol neben dem Spaltennamen, um die Spalte obligatorisch zu machen. Benutzer können eine obligatorische Spalte verschieben, können sie jedoch nicht entfernen.

      Hinweis: Obligatorische Spalten werden in Rot angezeigt.

5. Klicken Sie auf "OK".

   Das Fenster "Meine Aufgaben" im Posteingang zeigt Tabellen in dem Format an, das Sie angegeben haben.

Definieren der Standardprozesszuordnung für das Universum

Um Prozesszuordnungen zu CA RCM-Geschäfts-Workflows innerhalb eines Universums zuzuweisen, verwenden Sie die Registerkarte "Standardprozesszuordnung" unter "Einstellungen des Universums". CA RCM verwendet die Prozesse, die angegeben wurden, um Geschäfts-Workflows zu implementieren.

Beachten Sie Folgendes:

- Universums-Zuordnungen überschreiben globale Standardzuordnungen, die unter "Verwaltung", "Workflow-Einstellungen" festgelegt wurden.
- Sie können diese Standardzuweisungen überschreiben, wann Sie eine spezifische Prozesszuordnung auf einen Workflow anwenden. Führen Sie dies im CA RCM-Portal unter "Verwaltung", "Workflow-Einstellungen", "Workflow-Prozesszuordnungen" durch.

Um eine Universumsstandardprozesszuordnung zu bearbeiten, klicken Sie auf die Registerkarte "Standardrprozesszuordnung". Diese Registerkarte enthält die folgenden Abschnitte:

Zertifizierungskampagne

Listet Geschäfts-Workflows auf, die sich auf Zertifizierungskampagnen beziehen.

Anfrage nach Zugriff

Listet Geschäfts-Workflows auf, die sich auf Self-Service-Anfragen beziehen

Änderungsgenehmigung

Listet Geschäfts-Workflows auf, die sich auf Konfigurationsänderungen beziehen, die von CA RCM-Client-Tools ausgelöst wurden.

Jede Zeile stellt einen Typ von Geschäftsworkflow dar. Eine Dropdown-Liste zeigt verfügbare Prozesszuordnungen für diesen Typ von Workflow an.

Im Voraus genehmigte Verletzungen

Um bei Compliance- und Musterüberprüfungen spezifische Verletzungen auszugrauen oder zu ignorieren können Sie Im Voraus genehmigte Verletzungen innerhalb eines spezifischen Universums hinzufügen. Im Voraus genehmigte Verletzungen werden in den Fenstern zu Verletzungen in Kampagnen oder bei Self-Service angezeigt.

Für im Voraus genehmigte Verletzungen können Sie ein Ablaufdatum angeben. Sobald das Datum abläuft, gilt die Verletzung nicht mehr als im Voraus genehmigt und wird wie eine normale Verletzung eingestuft. Sie können auch einen Kommentar hinzufügen, um die Genehmigung der Verletzung zu erklären.

Wenn eine im Voraus genehmigte Verletzung ein Ablaufdatum oder einen Kommentar hat, erscheinen diese Angaben in der QuickInfo der Verletzung, wenn Sie die Maustaste über die Verletzung setzen.

Eine geplante Aufgabe wird in einem konfigurierbaren Intervall ausgeführt, durchsucht alle Universen, die eine genehmigte Auditkarte haben, und löscht alle abgelaufenen Warnungen.

Hinzufügen von im Voraus genehmigten Verletzungen

Für jedes Universum können Sie Verletzungen festlegen als Voraus genehmigt festlegen. Diese im Voraus genehmigten Verletzungen werden in Auditkarten für Compliance- und Musterüberprüfungen ausgeblendet (ignoriert) oder ausgegraut.

Hinweis: Sie benötigen Administrator-Berechtigungen im CA RCM-Portal, um diesen Vorgang auszuführen.

So fügen Sie im Voraus genehmigte Verletzungen hinzu

1. Stellen Sie in DNA die Verbindung mit dem CA RCM-Server her.
2. Öffnen Sie die Auditkarte, die Verletzungen enthält, die Sie im Voraus genehmigen wollen.

   Hinweis: Eine Verletzung muss in die Datenbank gespeichert werden, bevor Sie sie als im Voraus genehmigt festlegen können.

3. (Optional) Geben Sie wie folgt ein Ablaufdatum oder einen Kommentar an:
   a. Klicken Sie mit der rechten Maustaste auf die Verletzung, und wählen Sie "Bearbeiten".
   b. Wenn Sie ein Ablaufdatum angeben möchten, aktivieren Sie das Kontrollkästchen "Ablaufdatum" und geben Sie ein Datum ein.
   c. Wenn Sie einen Grund für die im Voraus genehmigte Verletzung angeben möchten, gehen Sie zum Kommentarfeld für im Voraus genehmigte Verletzungen und geben Sie den Text ein.
   d. Klicken Sie auf "OK".
4. Klicken Sie mit der rechten Maustaste auf die Verletzung, die Sie im Voraus genehmigen möchten, und wählen Sie "Diese Verletzung immer genehmigen" aus.
5. Vergewissern Sie sich, dass die Verletzung in der Auditkarte mit dem Namen "*Universum_Name* - Im Voraus genehmigte Verletzungen" enthalten ist.

Konfigurieren von im Voraus genehmigten Verletzungen

Wenn Sie einem Universum im Voraus genehmigte Verletzungen hinzufügen, können Sie angeben, ob die Verletzung ausgegraut oder ganz ignoriert (ausgeblendet) wird. Im Voraus genehmigte Verletzungen können unter "Einstellungen des Universums" konfiguriert werden.

So konfigurieren Sie im Voraus genehmigte Verletzungen

1. Gehen Sie im CA RCM-Portal auf "Verwaltung" und danach auf "Einstellungen".
2. Klicken Sie auf "Einstellungen des Universums".
3. Suchen Sie das Universum mit den im Voraus genehmigten Verletzungen für die Konfiguration und klicken Sie auf "Bearbeiten".

   Das Fenster "Bearbeiten" wird für das Universum angezeigt.
4. Wählen Sie neben "Genehmigte Warnungen sind:" die Anzeigekonfiguration aus, die Sie für im Voraus genehmigte Verletzungen möchten.

   Standard: ausgegraut
5. Klicken Sie auf "Speichern".

Konfigurieren von Reinigungsaufgaben für abgelaufene, im Voraus genehmigte Verletzungen

In CA RCM können Sie eine geplante Aufgabe aktivieren oder deaktivieren, um alle Universen zu durchsuchen, die eine genehmigte Auditkarte haben, und alle abgelaufenen Warnungen zu löschen. Diese geplante Aufgabe kann bei der Verwendung des CA RCM-Portals konfiguriert werden.

So konfigurieren Sie geplante Aufgaben, um abgelaufene Verletzungen zu löschen

1. Gehen Sie im CA RCM-Portal auf "Verwaltung" und danach auf "Einstellungen".
2. Klicken Sie auf "Eigenschaftseinstellungen".

3. Klicken Sie auf "Bearbeiten" und ändern Sie eine der beiden folgenden Einstellungen:
   - audit.delete.expired.alerts.enabled – aktiviert oder deaktiviert die Reinigung der abgelaufenen, im Voraus genehmigten Verletzungen

     Standard: Wahr (aktiviert)
   - audit.delete.expired.alerts.interval.seconds – Intervall in Sekunden zwischen den Reinigungen

     Standard: 86400 (ein Tag)

   Hinweis: Wenn Sie sich über das Standardverhalten für ein bestimmtes Universum hinwegsetzen wollen, erstellen Sie eine universumsspezifische Eigenschaft, zum Beispiel können Sie die Eigenschaft "universe.property.*Universum* \ *Name*.audit.delete.expired.alerts.enabled" erstellen und entsprechend für das Universum festlegen. Leerstellen in einem Universumsnamen werden durch einen umgekehrten Schrägstrich, gefolgt von einer Leerstelle ersetzt (\ ).
4. Klicken Sie auf "Speichern".

Standardmäßig enthalten Webservices keine im Voraus genehmigte Verletzungen. Wenn Sie im Voraus genehmigte Verletzungen einschließen wollen, legen Sie die folgende Eigenschaft fest:

```
audit.approved.alerts.webservices.include=true
```

Wenn Sie sich über das Standardverhalten für ein bestimmtes Universum hinwegsetzen möchten, erstellen Sie eine universumsspezifische Eigenschaft und legen Sie sie wie folgt auf "Wahr" fest:

```
universe.property.Mein\ Universum\
Name.audit.approved.alerts.webservices.include=true
```

Hinweis: Leerstellen in einem Universumsnamen werden durch einen umgekehrten Schrägstrich, gefolgt von einer Leerstelle ersetzt (\ ).

Anwendungsfall: Im Voraus genehmigte Verletzungen

Einige Personen der Personalabteilung müssen während eines arbeitsintensiven Zeitraums am Jahresende in der Finanzabteilung aushelfen.

Dazu benötigen die Angestellten der Personalabteilung Zugriff auf Finanzressourcen, was normalerweise eine Verletzung innerhalb von CA RCM generieren würde.

Sobald die Mitarbeiter der Personalabteilung Zugriff auf die Finanzressourcen haben, können Sie auf Compliance testen, und die sich daraus ergebenden Verletzungen der Liste der im Voraus genehmigten Verletzungen hinzufügen. Legen Sie abschließend das Ablaufdatum der im Voraus genehmigten Verletzung auf den ersten Tag des nächsten Jahres fest.

Hinweis: Stellen Sie sicher, dass Sie den geplanten Job aktivieren, der abgelaufene, im Voraus genehmigte Verletzungen löscht.

Alle durch diese vorübergehende Arbeitssituation generierten Verletzungen werden bis Jahresende unterdrückt. Abhängig von den Einstellungen des Universums werden diese Verletzungen in Kampagnentickets bzw. in mit dem Universum verknüpften Fenstern zur Self-Service-Validierung ausgeblendet oder grau unterlegt.

Informationen zu Benutzerkonten

In vielen Umgebungen bestimmen die Benutzerkonten verschiedener Endpunkte den Benutzerzugriff auf Ressourcen. Sie können diese Kontoinformationen in spezielle Kontokonfigurationsdateien im Universum importieren.

Die Kontokonfigurationen basieren auf den Master- und Modellkonfigurationen des Universums. Benutzer werden ihren Konten auf Bereitstellungsendpunkten zugewiesen.

Die Kontokonfigurationen werden automatisch erstellt, wenn Sie Kontoinformationen importieren. Diese Konfigurationsdateien werden nach den folgenden Konventionen benannt:

*modellkonfig*_Konten.cfg
*masterkonfig*_Konten.cfg

Hinweis: *modellkonfig* ist der Name der Modellkonfiguration im Universum. *masterkonfig* ist der Name der Masterkonfiguration im Universum.

Wenn Sie den Entitäten-Browser verwenden, um eine Konfiguration eines Universums zu prüfen, das Kontokonfigurationen enthält, zeigt der Entitäten-Browser Kontoinformationen für jeden Benutzer an.

CA RCM-Import von Kontoinformationen aus Identity Manager-Endpunkten

CA RCM kann Kontoinformationen aus Identity Manager-Endpunkten importieren. Wenn Sie einen Connector für Identity Manager erstellen, identifiziert der Importvorgang geänderte Kontoinformationen und aktualisiert die Kontokonfigurationen mit den Master- und Modellkonfigurationen des Universums.

Hinweis: Kontoinformationen werden nur abgerufen, wenn Sie einen Connector über das CA RCM-Portal importieren. Wenn Sie den Import über CA RCM-Data Management ausführen, werden in CA RCM keine Kontoinformationen abgerufen. Weitere Informationen zum Connector für Identity Manager finden Sie im *Connector für CA Identity Manager-Handbuch*.

Implizite Konten

Wenn ein Universum keine Kontokonfigurationen hat oder ein Benutzer über keine Konten auf externen Endpunkten verfügt, sind Kontoinformationen nicht verfügbar. CA RCM erstellt ein implizites Konto, um Ressourcen auf Benutzer zu beziehen, sogar wenn Kontoinformationen von externen Endpunkten nicht verfügbar sind.

Die folgenden Systemparameter kontrollieren implizite Konten:

implicit.accounts.enabled

Gibt an, ob CA RCM implizite Konten für Benutzer erstellt.

Gültige Werte: True, False (Wahr, Falsch)

Standard: True (Wahr)

implicit.accounts.field.name

Gibt das Feld der Benutzerdatensätzen an, das verwendet wird, um implizite Konten zu benennen. Normalerweise handelt es sich hierbei um das Feld "Anmelde-ID".

implicit.accounts.field.name.*Universum*

Gibt das Feld der Benutzerdatensätzen an, das verwendet wird, um implizite Konten im angegebenen Universum zu benennen. Dieser Wert überschreibt den Wert der Eigenschaft "implicit.accounts.field.name" für das angegebene Universum.

Universum

Definiert das Universum, welches das Feld verwendet, das implizite Konten benennt.

Implizite Konten sind wie folgt strukturiert:

- Der Kontoname wird aus dem in der Eigenschaft "implicit.accounts.field.name" angegebenen Feld übernommen.
- Der standardmäßig zugeordnete Endpunkt wird aus dem für das Universum angegebenen Feld der Ressourcen-Anwendung der Konfiguration genommen.

Importieren von CSV-Daten in eine Kontokonfiguration

Sie können Kontoinformationen aus einer Datei mit durch Kommas getrennten Werten (CSV) in eine spezielle Konfiguration importieren, die mit der Modellkonfiguration des Universums vergleichbar ist.

Hinweis: Da der dateibezogene Import ein einmaliger Prozess ist, verwenden Sie CSV-Dateien nur für anfängliche Importe oder gelegentliche administrative Aktualisierungen zu Kontoinformationen. Damit Kontoinformationen immer auf dem aktuellsten Stand sind, definieren Sie einen Datenconnectorjob, der Kontoinformationen regelmäßig aus Endpunkten importiert.

Hinweis: Sie benötigen Administrator-Berechtigungen im CA RCM-Portal, um diesen Vorgang auszuführen.

So importieren Sie CSV-Daten in eine Kontokonfiguration

1. Bereiten Sie die Datendatei vor.
2. Klicken Sie im Hauptmenü des CA RCM-Portals auf "Verwaltung" und anschließend auf "Konten".

   Das Fenster "Konten importieren" wird angezeigt.
3. Geben Sie das Zieluniversum und die CSV-Datei für den Import an, und klicken Sie auf "Import".

   CA RCM kopiert neue, eindeutige Datensätze aus der CSV-Datei in die Kontokonfigurationen. Vorhandene Informationen in den Kontokonfigurationen werden bewahrt.
4. (Optional) Um importierte Kontodaten zu überprüfen, öffnen Sie die Modellkonfiguration im Entitäten-Browser oder die Kontokonfigurationen in der Anwendung zur Datenverwaltung.

Struktur der CSV-Datei

Jeder Datensatz der CSV-Konten muss die folgenden Felder enthalten:

Personen-ID

Definiert den Benutzer im Zieluniversum, der Eigentümer des importierten Kontos ist. Dieses Feld stimmt in Inhalt und Format mit dem Feld "Personen-ID" im Universum überein.

Endpunkt

Definiert den Namen des Endpunkts, der Host für das Konto ist. Dieses Feld stimmt in Inhalt und Format mit dem Feld "Konfigurationsressourcen-Anwendung" des Universums überein.

Konto

Definiert den Kontonamen, wie er auf dem Endpunkt angegeben wurde.

Die erste Zeile der CSV-Datei muss wie folgt lauten:

```
Personen-ID,Endpunkt,Konto
```

Jede Zeile der Datei muss drei Werte enthalten, die durch Kommas getrennt sind.

Beispiel: Datendatei der CSV-Konten

Das folgende Beispiel zeigt eine CSV-Datei mit vier Datensätzen: Die ersten zwei Datensätze ordnen Konten zum gleichen Benutzer, John Meade, zu:

```
Personen-ID,Endpunkt,Konto
5467238,UNXMARKT,jmeade
5467238,NT-Security,john_meade
7635097,RACFTEST,marcus432
6523876,NT-Security,kim_bell
```

Kapitel 5: Verwenden von Geschäfts-Workflows

Dieses Kapitel enthält folgende Themen:

Geschäfts-Workflows in CA RCM

Ein *Geschäfts-Workflow* ist eine Reihe von zusammenhängenden Aufgaben, die eine Geschäftsanforderung erfüllen, wie z. B. die Zertifizierung von Benutzerberechtigungen oder das Anfordern von Genehmigungen für Berechtigungsänderungen.
Geschäfts-Workflows implementieren die Vorgänge eines Unternehmens zur Bestimmung der Compliance mit internen und externen Richtlinien in CA RCM. Die Implementierung dieser Vorgänge in CA RCM kann helfen sicherzustellen, dass ein Unternehmen eine zuverlässige und wiederholbare Methode zur Validierung der Compliance hat.

Zum Beispiel will ein Unternehmen ein vierteljährliches Audit über den Zugriff seiner Mitarbeiter auf Unternehmensressourcen ausführen. Der oder die Zuständige für Compliance eröffnet eine Zertifizierungskampagne, die erfordert, dass Manager die Berechtigungen ihrer direkten Mitarbeiter zertifizieren. Der Zuständige für Compliance verlangt außerdem, dass Ressourceneigentümer abgelehnte Berechtigungen für die Ressourcen genehmigen, die sie verwalten. In diesem Beispiel stellen die Zertifizierung und die Genehmigungsschritte einen Geschäfts-Workflow dar. Das Unternehmen kann diesen Workflow vierteljährlich einleiten oder häufiger, falls erforderlich.

Sie können Geschäfts-Workflows für die folgenden Aktivitäten in CA RCM definieren:

- Zertifizierungskampagnen
- Self-Service-Anfragen, wie z. B die eines Managers, der eine Berechtigungsänderung für einen Mitarbeiter anfordert oder eine Änderung in den Rollen, die die Mitarbeiter innehaben.

  Hinweis: Self-Service-Anfragen werden durch das Rollenverwaltungsmenü im Portal eingeleitet.

- Genehmigungsanforderungen für durch DNA-Client-Tools vorgenommene Änderungen am Rollenmodell

Aktionen, Aufgaben und Worflow-Prozesse

Ein Geschäfts-Workflow umfasst die folgenden Komponenten:

Aktion

Eine *Aktion* ist eine einzelne von einem Geschäftsteilnehmer in einem Workflow getroffene Entscheidung. Die gebräuchlichste Aktion für einen Manager oder Ressourceneigentümer besteht in der Genehmigung oder Ablehnung von Zugriffsrechten für Benutzer, Rollen oder Ressourcen-Entitäten. Andere Beispiele für Aktionen sind das Starten einer Zertifizierungskampagne oder die Beratung mit einem anderen Benutzer, bevor beschlossen wird, eine Berechtigung zu genehmigen oder abzulehnen.

Hinweis: Weitere Informationen über Aktionen finden Sie im Abschnitt Typen von Aktionen (siehe Seite 45).

Eine oder mehrere Aktionen stellen eine Aufgabe dar.

Aufgabe

Eine *Aufgabe* ist eine Reihe von Aktionen, die CA RCM-Benutzer abschließen müssen, um eine Anforderung in einem Geschäfts-Workflow zu erfüllen. Zum Beispiel enthält eine Kampagne zur Benutzerzertifizierung eine Aufgabe für jeden Benutzer, der überprüft wird. Jede Benutzerzertifizierungsaufgabe besteht aus Überprüfungsaktionen für jede Rolle oder Ressource, auf die der Benutzer zugreifen kann. CA RCM weist jede Aktion den entsprechenden Prüfern zu, verfolgt Antworten und implementiert etwaig erforderliche Änderungen.

Eine Aufgabe ist mit einem Workflow-Vorgang assoziiert.

Workflow-Prozess

Ein *Workflow-Vorgang* ist eine Reihe von Aktivitäten und Entscheidungspunkten in Workpoint-Prozessverwaltungssoftware (mit CA RCM installiert), die den Ablauf einer Aufgabe steuern. Ein Workflow-Vorgang ist mit einem Aufgabentyp in einem Geschäfts-Workflow assoziiert.

Hinweis: Aufgaben-Typen sind mit einem Standard-Workflow-Vorgang assoziiert. Wenn die Standard-Workflow-Vorgänge auf gewisse Geschäftsanforderungen nicht eingehen, können Systemadministratoren benutzerdefinierte Prozesse erstellen. Weitere Informationen finden Sie im *Programmierungshandbuch*.

Aktionstypen

CA RCM weist Aktionen Geschäftsteilnehmern zu. Die meisten Aktionen betreffen die Überprüfung eines Links, der eine Zugriffsberechtigung zwischen zwei Entitäten definiert. Normalerweise weist CA RCM eine Aktion einem Benutzer zu, der mit den Entitäten, die überprüft werden, in Zusammenhang steht, wie z. B. der Manager eines Benutzers oder der Verantwortliche einer Rolle oder Ressource.

Der Typ einer Aktion vermittelt eine allgemeine Vorstellung ihres Zweckes im Workflow sowie der Aufgabe, der sie enstammt. Die folgenden Typen von Aktionen werden in CA RCM-Geschäfts-Workflows verwendet:

Zertifizieren

Präsentiert einen vorhandenen Link zur Überprüfung. Die Ablehnung des Links zeigt an, dass eine Berechtigung entfernt werden sollte, und dass in der zugrunde liegenden CA RCM-Datenbank eine Änderung erforderlich ist. Normalerweise ist diese Aufgabe Teil der Anfangszertifizierungsphase in einem Zertifizierungskampagnen-Workflow.

Vorschlagen

Schlägt einen neuen Link für die in Überprüfung befindliche Entität vor. Die Genehmigung des Links zeigt an, dass eine Berechtigung hinzugefügt werden sollte, und dass in der zugrunde liegenden CA RCM-Datenbank eine Änderung erforderlich ist. Normalerweise ist diese Aufgabe Teil der Anfangszertifizierungsphase in einem Zertifizierungskampagnen-Workflow.

Genehmigen

Präsentiert einen neuen, geänderten oder gelöschten Link zur Genehmigung. Normalerweise ist diese Aufgabe Teil eines Self-Service-Workflows oder der Änderungsgenehmigungsphase in einem Zertifizierungskampagnen-Workflow. Wenn zum Beispiel ein Manager einen vorhandenen Link zwischen einem Benutzer und einer Ressource ablehnt, oder wenn er einen neuen Link zu der Ressource anfordert, müssen diese Änderungen vom Eigentümer der Ressource genehmigt werden.

Konsultieren

Präsentiert einen Link einem anderen Prüfer für dessen Empfehlung. Wenn Sie den Link in einer Konsultierungsaktion akzeptieren oder ablehnen, wird Ihre Entscheidung an den ursprünglichen Prüfer zurückgegeben. Sie können Ihre Wahl noch einmal überprüfen, bevor sie eine Entscheidung senden.

Andere/Benutzerdefiniert

Geschenke-Workflowsteuerelemententscheidungen oder andere von einem Prozess generierte benutzerdefinierte Aktionen.

Geschäfts-Workflow-Benutzer

Geschäfts-Workflows schließen die folgenden Typen von Aktivitäten ein, die unterschiedliche Typen von Benutzern in einem Unternehmen ausführen:

- Geschäfts-Workflows starten und verwalten

  Benutzer wie Compliance-Zuständige, Rolleningenieure, Rollen- und Ressourceneigentümer und Manager, initiieren Geschäfts-Workflows auf eine der folgenden Weisen:

  - Durchs Starten einer Zertifizierungskampagne
  - Durch Änderungen am Rollenmodell in DNA, die einer Genehmigungen bedürfen
  - Durch Anforderung einer Änderung an ihren Rollen oder den Rollen ihrer Angestellten

  Während eines Geschäfts-Workflows können diese Benutzer den Fortschritt der Aufgaben im Workflow überwachen.

- An Geschäfts-Workflow-Aufgaben teilnehmen

  Sobald ein Geschäfts-Workflow startet, weist CA RCM Benutzern wie Managern und Ressourceneigentümern Aktionen zu. Ein Beispiel für eine Aktion ist die Überprüfung von Benutzerberechtigungen und anderen Ressourcenlinks, und die Genehmigung bzw. Ablehnung derselben, je nach Bedarf.

  Je nachdem, welcher Workflow mit einer Aufgabe assoziiert ist, können diese Benutzer auch in der Lage sein, eine Aufgabe neu zuzuweisen oder sich mit anderen Benutzern zu beraten und weitere Informationen zu sammeln, bevor eine Berechtigung oder Ressourcenverknüpfung genehmigt oder abgelehnt wird.

- Geschäfts-Workflows anpassen

  CA RCM schließt Standard-Workflow-Vorgänge ein, die Administratoren zu Aufgaben in einem Geschäfts-Workflow zuordnen können. In einigen Fällen gehen die Standard-Workflow-Vorgänge nicht auf alle Geschäftsanforderungen ein. Systemintegratoren und andere fortgeschrittene Benutzer können Standardprozesse nach Bedarf anpassen. Zum Beispiel kann ein Systemintegrator einen benutzerdefinierten Workflow-Vorgang erstellen, um mehrere Genehmiger für einen gewissen Typ von Aufgabe zu unterstützen.

  Hinweis: Weitere Informationen zur Anpassung von Workflow-Vorgängen finden Sie im *Programmierungshandbuch*.

Das Portal bietet Geschäftsteilnehmern drei Schnittstellen an, um Geschäfts-Workflow-Aktivitäten anzuzeigen und abzuschließen:

- Das Fenster "Meine Anfragen", das im Posteingangsmenü verfügbar ist, ermöglicht es Managern und anderen Benutzern, Self-Service-Anfragen und andere Workflows zu verfolgen, die sie eingeleitet haben.
- Das Fenster "Meine Aufgaben", das im Posteingangsmenü verfügbar ist, unterstützt alle Benutzer, die an Workflows teilnehmen, mit einer persönlichen "To-Do"-Liste. Die Fenster "Meine Aufgaben" organisieren alle Aktionen, die CA RCM einer Person zuweist.
- Das Fenster "Workflows", das im Verwaltungsmenü verfügbar ist, ermöglicht es Administratoren, aktive Geschäfts-Workflows zu verfolgen und zu steuern.

Die Verfügbarkeit der Fenster "Workflow-Verwaltung", "Meine Anfragen" und "Meine Aufgaben" hängt von den für jedes Benutzerkonto auf dem CA RCM-Server definierten Berechtigungen ab. Normalerweise haben alle CA RCM-Benutzer eine Liste "Meine Aufgaben", aber nur Benutzer mit Berechtigungen auf Verwaltungsebene können auf die Workflow-Verwaltungsfenster zugreifen.

Geschäfts-Workflow-Prozess

Der folgende Prozess beschreibt die High-Level-Schritte in einem Geschäfts-Workflow:

1. CA RCM initiiert einen Geschäfts-Workflow, wenn eines der folgenden Ereignisse eintritt:
   - Ein Administrator startet eine Zertifizierungskampagne
   - Ein Manager oder ein anderer Geschäftsteilnehmer sendet eine Anfrage für eine Ressource oder eine Rolle
   - Ein Administrator nimmt Änderungen am DNA vor, wodurch sich das Rollenmodell ändert und ein Genehmigungsvorgang initiiert wird.

   Jeder Geschäfts-Workflow schließt eine Reihe von Aufgaben ein, die abgeschlossen werden müssen, bevor der Geschäfts-Workflow abgeschlossen wird.

   Jeder Typ von Aufgabe wird mit einem Workflow-Vorgang assoziiert, der die Aktionen und Entscheidungen definiert, die zum Abschließen der Aufgabe erforderlich sind.
2. CA RCM erstellt Aktionen für die am Geschäfts-Workflow beteiligten Benutzer im Fenster "Meine Aufgaben" im Portal und sendet E-Mails, um die Benutzer über ausstehende Arbeit zu benachrichtigen.
3. Die Benutzer sehen im Fenster "Meine Aufgaben" eine Liste ihrer Aktionen.

   Die Aktionen werden nach Entität gruppiert.

   Die Benutzer können jedes Element in der Liste öffnen, um die Aktionen anzuzeigen, die ihnen zugewiesen werden, Entscheidungen über jede Aktion zu treffen, oder um sich mit anderen Benutzern beraten.
4. Sobald alle Benutzer die für eine Aktion erforderliche Arbeit abgeschlossen haben, schreitet die Aktion zum nächsten Schritt fort oder wird abgeschlossen, so wie im Workflow-Vorgang definiert.

An einem Geschäfts-Workflow teilnehmen

Manager und andere Geschäftsteilnehmer im Unternehmen erhalten E-Mail-Benachrichtigungen, wenn ihnen CA RCM Aktionen zuweist. Wenn sie sich beim CA RCM-Portal anmelden, werden diese Aktionen in ihrem Fenster "Meine Aufgaben" aufgelistet.

In den meisten Fällen schließen Benutzer Aktionen in der interaktiven Anzeige ihres Fensters "Meine Aufgaben" ab.

Die Warteschlange "Meine Aufgaben" zeigt z. B. für jeden Manager, der an einer Zertifizierungskampagne teilnimmt, eine persönliche Liste von Berechtigungslinks an, die er überprüfen muss. Jeder Manager gibt seine Überprüfungsentscheidungen an und sendet die abgeschlossenen Aktionen an CA RCM.

Abgeschlossene Workflow-Aktionen

Sie schließen Workflow-Aktionen im Fenster "Meine Aufgaben" ab. Sie können Ihre angeforderten Aktionen gleichzeitig abschließen oder einige Aktionen teilweise abschließen, deren Fortschritt speichern und sie zu einem späteren Zeitpunkt abschließen.

So schließen Sie Workflow-Aktionen ab

1. Gehen Sie im CA RCM-Portalhauptmenü auf "Posteingang", "Meine Aufgaben".

   Das Fenster "Meine Aufgaben" wird angezeigt. Dieses Fenster bietet eine Übersicht über die Aktionen, die Ihnen zugewiesen wurden.

   Die Tabellen gruppieren Aktionen aufgrund der in Überprüfung befindlichen Entität. So listet zum Beispiel die Tabelle "Rollenaufgaben" die Aktionen auf, die mit Benutzern, Ressourcen oder anderen Rollen, die mit Rollen verknüpft sind, in Zusammenhang stehen. Jede Zeile der Tabelle stellt eine Aktion oder eine Gruppe von Aktionen eines Typs, eines Workflows, für eine Rolle dar.

2. (Optional) Aktionen filtern, (siehe Seite 51) die angezeigt werden.

   Hinweis: Durch Filter wird festgelegt, welche Aktionen angezeigt werden. Sie legen nicht fest, welche Aktionen Ihnen zugewiesen werden. Durch einen Filter ausgeblendete Einträge bleiben aktiv.

3. Klicken Sie auf die Schaltfläche "Öffnen" neben einer Gruppe von Aktionen.

   Ein Aktionsdetailsfenster zeigt eine Aktion oder eine Gruppe von Aktionen eines Typs, aus einem Workflow, auf eine primäre Entität bezogen an. Der Titel des Fensters zeigt den Typ der Aktionen an, die in dem Fenster aufgelistet werden, sowie die primäre, in Überprüfung befindliche Entität. Zum Beispiel enthält ein Fenster von Benutzerzertifizierungsaktionen eine Tabelle von Rollen, die mit dem Benutzer verlinkt sind, und eine Tabelle von Ressourcen, die mit dem Benutzer verlinkt sind.

4. Verwenden Sie die Informationsfelder und interaktiven Optionen (siehe Seite 69) des Fensters, um Links zu überprüfen.

5. Die folgenden Entscheidungen schließen Ihre Bearbeitung einer Aktion ab:

   - Genehmigung des Links
   - Ablehnung des Links
   - Neuzuweisung der Aktion zu einem anderen Prüfer

   Hinweis: Sie können für Konsultierungsaktionen (siehe Seite 58) oder Workflow-Steuerungs-Aktionen (siehe Seite 52) andere Optionen wählen.

6. Führen Sie einen der folgenden Schritte aus:

   - Klicken Sie auf ‘Speichern’, um die Überprüfungsentscheidungen und andere Vorgänge, die Sie ausgeführt haben, zu speichern, ohne sie an CA RCM zu senden. CA RCM zeigt diese Entscheidungen das nächste Mal, wenn Sie sich am Portal anmelden, an.
   - Klicken Sie auf "Senden", um Ihre Entscheidungen an CA RCM zu senden. Abgeschlossene Aktionen werden aus Ihrer Warteschlange "Meine Aufgaben" entfernt.
   - Klicken Sie auf "Abbrechen", um zum Übersichtsfenster zurückzukehren, ohne Ihre Entscheidungen zu speichern.

   Das Übersichtsfenster "Meine Aufgaben" wird angezeigt.

Filtern der Warteschlange "Meine Aufgaben"

Sie können die angezeigten Aktionen im Fenster "Meine Aufgaben" filtern. Dies kann Ihnen dabei helfen, Ihre Arbeit zu organisieren. Zum Beispiel können Sie auf spezifische Workflows bezogene Aktionen identifizieren oder Überprüfungsaktionen des gleichen Typs in einer einzigen Sitzung bearbeiten.

Sie können auch Filter miteinander kombinieren. Zum Beispiel können Sie ausschließlich Konsultierungsaktionen anzeigen, die sich auf einen bestimmten Workflow beziehen.

So filtern Sie die Warteschlange "Meine Aufgaben"

1. Klicken Sie auf Schaltfläche "Filtern" im Kopf der Seite "Meine Aufgaben".

   Das Dialogfenster "Filteraktionen" wird angezeigt:

2. Wählen Sie Aktionen aus, die sich auf bestimmte Workflows beziehen.

   a. Wählen Sie die Option "Bestimmte Workflows" aus und klicken Sie auf das Plussymbol.

      Das Dialogfeld "Workflows auswählen" wird angezeigt.

   b. Wählen Sie unter "Verfügbaren Workflows" den Typ von Workflow aus, den Sie haben wollen, geben Sie ein Startdatum an und klicken Sie auf "Suchen".

      Die Tabelle listet Workflows auf, die mit den Suchkriterien übereinstimmen.

   c. Wählen Sie Workflows aus und klicken Sie auf den Pfeil "Hinzufügen".

      Die Workflows werden in der Liste "Ausgewählte Workflows" angezeigt.

   d. (Optional) Wiederholen Sie die Suche mit unterschiedlichen Bedingungen, und fügen Sie der Liste "Ausgewählte Workflows" weitere Workflows hinzu.

   e. Klicken Sie auf "OK", um den Filter zu definieren.

      Es werden nur Aktionen angezeigt, die sich auf die ausgewählten Workflows beziehen.

   Das Fenster "Filteraktionen" wird angezeigt:

3. Wählen Sie die anzuzeigenden Aktionstypen aus. Wählen Sie die Option "Alle" aus, um alle Typen von Aktionen auszuwählen oder um Ihre Auswahl zu löschen.

   Hinweis: Dieser Filter wird zusätzlich zu einem anderen, von Ihnen definierten Filter angewendet.

4. Wählen Sie die anzuzeigenden Aktionszustände aus. Folgende Optionen sind verfügbar:

   Ausstehend

   Aktionen, die Sie noch nicht an CA RCM gesendet haben.

   Abgeschlossen

   Aktionen, die Sie an CA RCM gesendet haben.

   Hinweis: Dieser Filter wird zusätzlich zu einem anderen, von Ihnen definierten Filter angewendet.

5. Klicken Sie auf "OK".

   Das Fenster "Meine Aufgaben" zeigt nur Aktionen an, die Ihren Filterkriterien entsprechen.

Allgemeine Aufgaben abschließen

Wenn Sie in der Tabelle "Allgemein" im Übersichtsfenster "Meine Aufgaben" auf "Öffnen" klicken, öffnet sich ein Fenster, das Aktionen anzeigt, die Sie ausführen können, um den Fortschritt des Workflow zu steuern.

Nur einige wenige der Aktionsinformationsfelder und Operationen (siehe Seite 69) sind relevant für diese Workflow-Steuerungsaktionen. Der Vorgang "Zugehörige Informationen anzeigen" zeigt den Fortschritt der zugehörigen Aufgaben und Aktionen im Workflow an. Diese Informationen können Ihnen dabei helfen, zu entscheiden, welche Steuerelementaktionen Sie ausführen sollten und wann.

Beispiel: Änderungsgenehmigungen in einer Zertifizierungskampagne starten

Standardmäßige CA RCM-Zertifizierungskampagnen haben eindeutige Zertifizierungs- und Änderungsgenehmigungsphasen. Genehmigungsaktionen für geänderte Links werden zurückgestellt, bis alle Zertifizierungsaktionen abgeschlossen sind.

Wenn eine Kampagne beginnt, erhält der Kampagneneigentümer eine Workflow-Steuerungsaktion. Die Aktion stoppt vorbereitenden Zertifizierungsaktionen und leitet Änderungsgenehmigungen ein.

Die für diese Aktion angezeigte "Zugehörige Information" zeigt den Fortschritt der Zertifizierungsphase für die Kampagne an.

Wenn der Kampagneneigentümer diese Workflow-Steuerungsaktion sendet, wird die Genehmigungsphase des Workflows gestartet, und unvollständige Zertifizierungsaktionen werden abgebrochen.

Beispiel: Neue Rolle erstellen

Wenn Benutzer neue Rollen anfordern, geben sie einen Eigentümer für die neue Rolle an.

Dieser Eigentümer erhält eine Workflow-Steuerungsaktion. Die Aktion genehmigt die Erstellung von der Rolle.

Die für diese Aktion angezeigte "Zugehörige Information" zeigt den Fortschritt von untergeordneten Aktionen an, die die Berechtigungen genehmigen, die mit der neuen Rolle assoziiert sind.

Wenn der Rolleneigentümer diese Workflow-Steuerungsaktion sendet, erstellt CA RCM die Rolle mit gegenwärtig genehmigten Berechtigungen. Berechtigungen, die noch nicht genehmigt sind, werden nicht in die neue Rolle aufgenommen.

Neu zuweisen von Links an andere Prüfer

Sie können Überprüfungsaktionen, die Ihnen CA RCM zuweist, auf einen anderen Prüfer übertragen. Optionen und Steuerelemente zur Neuzuweisung erscheinen in den Warteschlangen "Meine Aufgaben" und "Meine Anforderungen" sowie in den von Administratoren verwendeten Workflow-Verwaltungs-Fenstern.

Hinweis: Der CA RCM-Administrator kann diese Optionen und Steuerelemente im Portal selektiv aktivieren.

Um Aktionen in diesen Fenstern neu zuzuweisen, führen Sie einen der folgenden Schritte durch:

- Klicken Sie auf das Symbol "Neu zuweisen" neben einer Aktion oder Gruppe von Aktionen.
- Um alle Elemente in einer Tabelle neu zuzuweisen, aktivieren Sie das Kontrollkästchen im Spaltenkopf "Neu zuweisen" in der Tabelle.
- In den Fenstern "Meine Anforderungen" und Workflow-Verwaltungs-Fenstern:
    a. Klicken Sie auf das Prüfersymbol neben einem in Überprüfung befindlichen Link.
    b. Ein Dialogfeld listet alle Prüfer für diesen Link auf.
    c. Klicken Sie auf das Symbol "Neu zuweisen" neben den Prüfern, die Sie ändern wollen.

Wenn Sie eine Aktion oder Gruppe von Aktionen neu zuweisen, wird der Zielbenutzer neben der Symbol "Neu zuweisen" angezeigt. Die Aktion wird diesem Benutzer neu zugewiesen. Das Feld "Standardzuständiger" am unteren Fensterrand zeigt das Standardziel für neu zugewiesene Aktionen an.

Hinweis: In einigen Fenstern "Meine Anforderungen" ist der Standardprüfer der Workflow-Eigentümer oder dessen Manager.

Führen Sie einen der folgenden Schritte aus, um den Zielbenutzer zu ändern

- Klicken Sie auf das Feld "Standardzuständiger", um einen anderen Benutzer auszuwählen. Wenn Sie Aufgaben neu zuweisen, richten sie sich an den neuen Standardzuständigen.

  Hinweis: Der Zielbenutzer von früher neu zugewiesenen Aktionen ändert sich nicht, wenn Sie den Standardzuständigen ändern.
- Klicken Sie auf den Zielbenutzer eines individuellen Links, um seinen Wert zu ändern.

Entscheidungen über Neuzuweisungen werden gespeichert, wenn Sie in Ihrer Warteschlange "Meine Aufgaben" auf "Speichern" klicken. Wenn Sie auf "Senden" klicken, werden die Aktionen in die Warteschlange "Meine Aufgaben" des Zielbenutzers verschoben. Die neu zugewiesenen Links zählen bei Ihrem Fortschritt in der Bearbeitung von Aktionen mit.

So fügen Sie Kommentare, Dateien oder Links hinzu

Sie können an eine Aktion oder Gruppe von Aktionen Datendateien mit weiterführenden Informationen anhängen. Auf ähnliche Weise können Sie einer Aktion oder Gruppe von Aktionen Textkommentare hinzufügen.

Die folgenden Beispiele zeigen typische Anwendungen solcher Zusatzinformationen:

- Delegierung: Fügen Sie Daten oder Kommentare hinzu, wenn Sie die Aktion anderen Prüfern neu zuweisen.
- Konsultation: Wenn eine Überprüfungsaktion mit anderen Prüfern geteilt wird, können Sie Zusatzinformationen gemeinsam nutzen, um den Entscheidungsprozess zu unterstützen.
- Pflichtdokumentation: In einigen Kampagnen müssen Sie zwingend einen Kommentar zu Ihren Entscheidungen angeben. Zum Beispiel könnte es notwendig sein, zu begründen, warum ein Link, der die Geschäftspolitik verletzt, genehmigt wurde.

Jeder in Überprüfung befindliche Link hat eine Warteschlange für Kommentare und Warteschlange für Anhänge. Alle Kommentare und Anhänge sind für alle Entitätseigentümer, Berater und Prüfer sichtbar.

Sie können an eine Gruppe von Aktionen einen Kommentar oder eine Datei anhängen, wie z. B. die im Fenster "Meine Aufgaben" aufgelisteten Gruppen. In diesem Fall verbindet sich der Anhang mit der *üblichen Entität* der Gruppe. Wenn Sie zum Beispiel einen Kommentar an eine Gruppe von Links anhängen, die sich auf einen einzelnen Benutzer beziehen, wird der Kommentar mit diesem Benutzer verknüpft.

Anhängen eines Kommentars

Sie können einer Aktion oder Gruppe von Aktionen Textkommentare hinzufügen, die Ihnen oder anderen Prüfern nützliche Hinweise geben können.

So fügen Sie einen Kommentar hinzu

1. Klicken Sie auf das Symbol "Kommentar" neben einer Aktion, einer Gruppe von Aktionen oder einem sich in Überprüfung befindlichen Link.

   Das Popup "Kommentare" wird angezeigt.

2. Bearbeiten Sie Ihren Kommentar.
3. Klicken Sie auf "OK".

   Das Symbol "Kommentar" zeigt die Anzahl der Kommentare an.

Anhängen von Dateien

Um Überprüfungsentscheidungen zu unterstützen, können Sie Datendateien an eine Aktion oder Gruppe von Aktionen anhängen

So hängen Sie eine Datei an:

1. Klicken Sie auf das Symbol "Anhang" neben einer Aktion oder Gruppe von Aktionen.

   Das Popup "Anhänge" wird angezeigt.

2. Geben Sie eine Beschreibung ein und navigieren Sie zu einer Datei.
3. Klicken Sie auf "Hochladen".

   Dateiinhalte werden auf die CA RCM-Datenbank hochgeladen. Die Datei wird der Liste "Anhänge" als klickbarer Link hinzugefügt.

4. Klicken Sie auf "Schließen".

   Das Symbol "Anhang" zeigt die Anzahl der Anhänge an.

Beratung mit anderen Prüfern

Sie können sich mit anderen beraten, wenn Sie einen Link oder eine Entität überprüfen. Konsultierte Prüfer zeigen ihre Überprüfungsentscheidung an, und können Anmerkungen hinzufügen oder Dateien mit bekräftigenden Daten anhängen. Sie können diese Entscheidungen und bekräftigende Informationen anzeigen, wenn Sie Ihre eigene Entscheidung treffen.

So konsultieren Sie andere Prüfer

1. Klicken Sie in einem Aktionsdetailfenster auf das Symbol neben einem Link oder einer Workflow-Steuerungsaktion.

   Das Dialogfeld "Konsultierung" wird angezeigt.

2. Ausgewählte Consultants:

   a. Klicken Sie auf das Symbol mit dem Pluszeichen, um einen Consultant hinzuzufügen.

      Das Dialogfeld "Consultant auswählen" wird angezeigt.

   b. Verwenden Sie die Dropdown-Felder, um einen Filter zu definieren, und klicken Sie auf "Suche".

      CA RCM filtert die Liste von Benutzern.

c. Klicken Sie neben dem Benutzer, den Sie konsultieren möchten, auf "Auswählen", anschließend auf "Anwenden".

   Der Benutzer erscheint im Feld "An" des Dialogfelds "Konsultierung".

Wiederholen Sie diese Schritte, um zusätzliche Consultants auszuwählen.

Klicken Sie auf das Minussymbol neben einem Namen im Feld "An", um einen Consultant zu löschen.

3. (Optional) Geben Sie im Feld "Kommentar" eine kurze Nachricht an die Consultants ein.
4. Klicken Sie auf "Senden".

   CA RCM stellt eine Kopie der Aktion in die Warteschlange "Meine Aufgaben" eines jeden Consultants. Jede Konsultation wird in der Liste "Konsultierungsabfragen" angezeigt.
5. Klicken Sie auf "Schließen".

   Das Dialogfeld "Konsultierung" wird geschlossen. Das Konsultierungssymbol zeigt die Anzahl an Consultants und die Anzahl von Antworten an.
6. (Optional) Hängen Sie Dateien, Links oder zusätzliche Kommentare zur Aktion an. Consultants können diese unterstützende Information anzeigen.
7. Überwachen Sie die Aktion.

   Hinweis: Sie können Ihre Überprüfungsentscheidung jederzeit senden, gleichgülitg, ob Consultants antworten oder nicht. Wenn Sie Ihre Entscheidung senden, bevor ein Consultant antwortet, zeigt CA RCM die Aktion des Consultants als "abgebrochen" in den Workflow-Fortschritt (siehe Seite 68)-Diagrammen an.
8. Wenn das Konsultierungssymbol anzeigt, dass Consultants geantwortet haben, klicken Sie auf das Symbol.

   Das Feld "Ergebnis" zeigt die empfohlene Entscheidung jedes Prüfers an.

   Die Felder "Kommentar" und "Anhang" zeigen Kommentare oder von Consultants angehängte Dateien an.

   Hinweis: Wenn ein Berater die Konsultierungsaktion ablehnt, ohne zu antworten, bleibt das Feld "Ergebnis" leer.
9. Klicken Sie auf "Schließen".
10. Geben Sie im Aktionsdetailfenster Ihre Entscheidung für die Aktion an.

Handhabung von Konsultierungsaktionen

Andere Prüfer können Ihre Meinung über einen in Überprüfung befindlichen Link oder andere Aktionen anfordern. Diese Anforderungen werden in Ihrer Warteschlange "Meine Aufgaben" als Konsultierungsaktionen angezeigt.

Sie verarbeiten diese Aktionen wie Ihre eigenen Überprüfungsaktionen. Wenn Sie auf "Senden" klicken, zeigt CA RCM Ihre Entscheidung dem ursprünglichen Prüfer als eine Empfehlung an. Der ursprüngliche Prüfer trifft die endgültige Überprüfungsentscheidung.

Der ursprüngliche Prüfer kann Kommentare oder Anhänge einfügen, um Ihnen Anhaltspunkte zu geben. Auf ähnliche Weise können Sie Kommentare oder Anhänge hinzufügen, um Ihre Empfehlung zu bekräftigen.

In zusätzlichen Überprüfungsoptionen ist für Konsultierungsaktionen die folgende Option verfügbar:

Schließen

Entfernt eine Konsultierungsaktion aus der Warteschlange "Meine Aufgaben", ohne dem ursprünglichen Prüfer zu antworten. Dies bedeutet so viel, wie die Konsultierung abzulehnen. Kommentare oder Anhänge, die Sie dem in Überprüfung befindlichen Link hinzufügen, sind für die anderen Prüfer sichtbar.

Spalten in Tabellen "Meine Aufgaben" anpassen

Sie können die Tabellen-Layouts anpassen, die CA RCM verwendet, um Workflow-Aktionen anzuzeigen.

Obligatorische Spalten können nicht aus Tabellenansichten entfernt werden. Roter Text und ein gesperrtes Schlosssymbol zeigen obligatorische Spalten in Benutzeranpassungsfenstern und Dialogfeldern an. Einige obligatorische Spalten sind hartkodierte Standards in CA RCM. Administratoren können zusätzliche obligatorischen Spalten definieren.

So passen Sie Spalten in Tabellen "Meine Aufgaben" an

1. Klicken Sie auf dem Tabellenkopf, den Sie ändern wollen, auf "Anpassen".

   Das Dialogfeld "Anpassen" wird angezeigt.

2. Verwenden Sie die Pfeiltasten, um Spalten hinzuzufügen oder zu entfernen, und um die Spalten anzuordnen.

Hinweis: Obligatorische Spalten werden in Rot angezeigt. Sie können diese Spalten nicht aus der Tabelle entfernen.

3. Klicken Sie auf "OK".

   CA RCM zeigt Aufgaben oder Aktionen für diese Entität in dem Tabellenformat an, das Sie angegeben haben.

Verwalten von Anforderungen

Manager und andere Geschäftsteilnehmer können Workflows initiieren, indem sie eine Berechtigungsänderung für einen Mitarbeiter anfordern oder Änderungen an Rollen, die sie besitzen.

Die Fenster "Meine Anforderungen" im Posteingangsmenü ermöglicht es diesen Benutzern, den Fortschritt ihrer Anforderungen zu überwachen.

Filtern der Workflow-Liste

Sie können die Liste Workflows filtern, um spezifische Workflows oder Gruppen von Workflows einfacher zu finden.

So filtern Sie die Workflow-Liste

1. Klicken Sie auf "Filter" in der Kopfzeile.

   Das Dialogfeld "Workflows filtern" wird angezeigt.

2. Definieren Sie die Filterkriterien wie folgt:

   Fälligkeitsdatum

   Verwenden Sie die Felder "Von" und "Bis", um einen Zeitraum anzugeben. Der Filter wählt Workflows mit einem Fälligkeitsdatum innerhalb dieses Zeitraums aus.

   Workflow-Typen

   Wählen Sie die anzuzeigenden Workflow-Typen aus. Wählen Sie die Option "Alle" aus, um alle Typen von Workflows auszuwählen oder um Ihre Auswahl zu löschen.

   Workflow-Status

   Wählen Sie die anzuzeigenden Workflow-Status aus. Wählen Sie die Option "Alle" aus, um alle Status auszuwählen oder um Ihre Auswahl zu löschen. Der Filter wählt Workflows aus, die gegenwärtig in den angegebenen Status sind.

   Hinweis: Sie können diese Filterkriterien miteinander kombinieren.

3. Klicken Sie auf "OK".

   Die Liste zeigt nur Workflows an, die Ihren Filterkriterien entsprechen.

Anforderungen überwachen

Verwenden Sie die Schnittstelle "Meine Anforderungen", um Geschäftsabläufe, die Sie eingeleitet haben, zu überwachen.

So überwachen Sie Ihre CA RCM-Workflows

1. Gehen Sie im CA RCM-Portalhauptmenü auf "Posteingang", "Meine Anforderungen".

   Das Fenster listet die aktiven Workflows auf, die Sie eingeleitet haben. Sie können die in der Tabelle angezeigten Felder anpassen (siehe Seite 58).

2. (Optional) Filtern Sie die in der Liste angezeigten Workflows (siehe Seite 59).
3. Klicken Sie auf eine Rolle, um die Details anzuzeigen.

   Das Fenster mit den Workflow-Details wird angezeigt. Es enthält die folgenden Registerkarten:

   - Übersicht - Zeigt den Fortschritt des Ablaufs in Grafiken und Diagrammen an. Diese Registerkarte wird standardmäßig geöffnet.
   - Workflow-Fortschritt nach betroffenen Entitäten - Listet Aufgaben nach in Überprüfung befindlichen Entitäten in jeder Aufgabe auf und zeigt ihren Fortschritt.
   - Workflow-Fortschritt nach Prüfern - Listet Aktionen nach deren Prüfern auf und zeigt ihren Fortschritt.
4. (Optional) Klicken Sie auf "Anpassen", um die Diagramme der Registerkarte "Übersicht" zu ändern.
5. Klicken Sie auf eine der Registerkarten "Workflow-Fortschritt".

   Aktionen werden in Gruppen aufgelistet. Die Tabelle zeigt den Fortschritt einer jeden Gruppe.

   Hinweis: Wenn der Inhalt und Umfang des Workflows groß ist, oder zusätzliche große Workflows aktiv sind, aktualisieren sich die Statusanzeigen unter Umständen nicht sofort. Es kann einige Minuten dauern, bis gesendete Aktionen in den Statusanzeigen als vollständig ausgeführt angezeigt werden.
6. Klicken Sie auf die Schaltfläche "Öffnen" neben einer Gruppe.

   Eine Tabelle listet Aktionen in der Gruppe auf.
7. Klicken Sie auf die Schaltfläche "Öffnen" oder das Symbol "Prüfer".

   Ein Aktionsdetailsfenster zeigt eine Aktion oder eine Gruppe von Aktionen eines Typs, aus einem Workflow, auf eine primäre Entität bezogen an.

   Aktionen, die schon an CA RCM gesendet wurden, werden verdunkelt.
8. Verwenden Sie die Informationsfelder und interaktiven Optionen (siehe Seite 69) des Fensters, um Links zu überprüfen.

   Für Aktionen, die anderen zugewiesen sind, sind nur die Vorgänge "Neu zuweisen", "Kommentar" und "Anhang" verfügbar.

   Die Optionen "Genehmigen" und "Ablehnen" sind nur verfügbar für Aktionen, die Ihnen zugewiesen sind.

9. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie auf "Senden", um Ihre Entscheidungen an CA RCM zu senden.
   - Klicken Sie auf "Abbrechen", um zum Übersichtsfenster zurückzukehren, ohne Ihre Entscheidungen zu speichern.

Workflow-Fortschritt nach Entitäten oder Prüfern anzeigen

Das Fenster "Meine Anforderungen" und die "Workflows"-Fenster bieten zwei Methoden, den Fortschritt eines Workflow anzuzeigen.

- Die Registerkarte "Workflow-Fortschritt nach betroffenen Entitäten" gruppiert *Aufgaben* des Workflows nach den in Überprüfung befindlichen Entitäten einer jeden Aufgabe. Die Einträge in diesen Tabellen sind Aufgaben, die von CA RCM für den Workflow generiert wurden, und zwar basierend auf dem Workflowtyp, der Grundkonfiguration, des Umfangs der in Überprüfung befindlichen Entitäten und anderen Einstellungen.
- Die Registerkarte "Workflow-Fortschritt nach Prüfer" gruppiert *Aktionen des Workflows* zugewiesenen Prüfern und zeigt ihren Fortschritt. Die Einträge in diesen Tabellen sind Aktionen, die von den Workpoint-Jobs, die die Aufgaben des Workflows implementieren, generiert wurden.

Wenn ein Workflow in Bearbeitung ist, können Sie von jeder Registerkarte aus ein Drilldown durchführen, um individuelle Aktionen anzuzeigen. Die Registerkarte "Workflow-Fortschritt nach betroffenen Entitäten" zeigt von CA RCM erstellte High-Level-Aufgaben an. Die Hauptansichten dieser Registerkarte werden aufgefüllt, wenn CA RCM seine Analyse der in Überprüfung befindlichen Links im Workflow abschließt.

Jede dieser Aufgaben löst zahlreiche Workpoint-Jobs aus, wenn sie implementiert werden. Die Registerkarte "Workflow-Fortschritt nach Prüfer" zeigt die sich ergebenden Low-Level-Workpoint-Jobs an, sowie die Prüfer, die jedem Link zugewiesen wurden. Diese Registerkarte wird nur aufgefüllt, wenn Workpoint-Jobs initiiert werden, und ihr Inhalt hängt von der für jede Aufgabe durch den entsprechenden Workpoint-Prozess implementierten Logik ab.

Geschäfts-Workflows verwalten

Rolleningenieure und -administratoren verwenden das Fenster "Workflows", um Kampagnen und andere aktive CA RCM-Workflows zu verfolgen und zu steuern.

Die Workflow-Fenster ähneln den Fenstern "Meine Anforderungen"; allerdings bieten sie zusätzliche Verwaltungs- und Steuerungsmöglichkeiten, die in den Fenstern "Meine Anforderungen" nicht zur Verfügung stehen.

Um dieses Fenster zu verwenden, müssen Benutzer Admin-Berechtigungen im CA RCM-Portal haben.

So verwalten Sie Geschäfts-Workflows

1. Gehen Sie im CA RCM-Portalhauptmenü auf "Verwaltung", "Workflows".

   Das Fenster listet die aktiven CA RCM-Workflows auf. Wenn ein Workflow endet, wird er aus der Liste entfernt.

2. (Optional) Passen Sie (siehe Seite 58)die in der Tabelle angezeigten Informationsfelder an.

3. (Optional) Filtern Sie die in der Tabelle angezeigten Workflows (siehe Seite 59).

4. Klicken Sie auf eine Rolle, um die Details anzuzeigen.

   Das Fenster mit den Workflow-Details wird angezeigt. Es enthält die folgenden Registerkarten:

   - Übersicht - Ein Dashboard zeigt den Fortschritt des Ablaufs in Grafiken und Diagrammen an. Diese Registerkarte wird standardmäßig geöffnet.
   - Verwaltung - bietet erweiterte Workflow-Steuerungsoptionen, um den Workflow anzuhalten oder neu zu starten, oder um Eskalations-E-Mails (siehe Seite 66)aufgrund nicht abgeschlossener Aktionen zu senden.
   - Workflow-Fortschritt nach betroffenen Entitäten - Listet Aufgaben nach in Überprüfung befindlichen Entitäten in jeder Aufgabe auf und zeigt ihren Fortschritt.
   - Workflow-Fortschritt nach Prüfern - Listet Aktionen nach deren Prüfern auf und zeigt ihren Fortschritt.

5. Verwalten Sie Workflow-Aufgaben und Aktionen im Detail:

   a. Klicken Sie auf eine der Registerkarten "Workflow-Fortschritt".

      Aktionen werden in Gruppen aufgelistet. Die Tabelle zeigt den Fortschritt einer jeden Gruppe.

      Hinweis: Wenn der Inhalt und Umfang des Workflows groß ist, oder zusätzliche große Workflows aktiv sind, aktualisieren sich die Statusanzeigen unter Umständen nicht sofort. Es kann einige Minuten dauern, bis gesendete Aktionen in den Statusanzeigen als vollständig ausgeführt angezeigt werden.

   b. Klicken Sie auf die Schaltfläche "Öffnen" neben einer Gruppe.

      Eine Tabelle listet Aktionen in der Gruppe auf.

   c. Klicken Sie auf die Schaltfläche "Öffnen" oder auf das Symbol "Prüfer", um mehr Details zu erhalten.

   Ein Aktionsdetailsfenster zeigt eine Aktion oder eine Gruppe von Aktionen eines Typs, aus einem Workflow, auf eine primäre Entität bezogen an.

   Aktionen, die schon an CA RCM gesendet wurden, werden verdunkelt.

6. Verwenden Sie die Informationsfelder und interaktiven Optionen (siehe Seite 69) des Fensters, um Links zu überprüfen.

   Für Aktionen, die anderen zugewiesen sind, sind nur die Vorgänge "Neu zuweisen", "Kommentar" und "Anhang" verfügbar.

   Die Optionen "Genehmigen" und "Ablehnen" sind nur verfügbar für Aktionen, die Ihnen zugewiesen sind.

7. Führen Sie einen der folgenden Schritte aus:

   - Klicken Sie auf "Senden", um Ihre Entscheidungen an CA RCM zu senden.
   - Klicken Sie auf "Abbrechen", um zum Übersichtsfenster zurückzukehren, ohne Ihre Entscheidungen zu speichern.

Filtern der Workflow-Liste

Sie können die Liste Workflows filtern, um spezifische Workflows oder Gruppen von Workflows einfacher zu finden.

So filtern Sie die Workflow-Liste

1. Klicken Sie auf "Filter" in der Kopfzeile.

   Das Dialogfeld "Workflows filtern" wird angezeigt.

2. Definieren Sie die Filterkriterien wie folgt:

   Fälligkeitsdatum

   Verwenden Sie die Felder "Von" und "Bis", um einen Zeitraum anzugeben. Der Filter wählt Workflows mit einem Fälligkeitsdatum innerhalb dieses Zeitraums aus.

   Workflow-Typen

   Wählen Sie die anzuzeigenden Workflow-Typen aus. Wählen Sie die Option "Alle" aus, um alle Typen von Workflows auszuwählen oder um Ihre Auswahl zu löschen.

   Workflow-Status

   Wählen Sie die anzuzeigenden Workflow-Status aus. Wählen Sie die Option "Alle" aus, um alle Status auszuwählen oder um Ihre Auswahl zu löschen. Der Filter wählt Workflows aus, die gegenwärtig in den angegebenen Status sind.

   Hinweis: Sie können diese Filterkriterien miteinander kombinieren.

3. Klicken Sie auf "OK".

   Die Liste zeigt nur Workflows an, die Ihren Filterkriterien entsprechen.

Verwaltung von Workflows in der Registerkarte "Verwaltung"

Sie können Geschäfts-Workflows in der Registerkarte "Verwaltung" der Workflow-Fenster verwalten; diese befinden sich im Verwaltungsmenü. In der Registerkarte "Verwaltung" können Sie allgemeine Workflow-Information überprüfen und einen Workflow starten, anhalten oder archivieren. Diese Registerkarte enthält die folgenden Optionen:

Workflow starten

Startet eine Kampagne, die mit der Option "Deaktiviert" erstellt wurde.

Workflow anhalten

Hält einen Workflow an. Aktionen dieses Workflows werden in der Warteschlange "Meine Aufgaben" der Teilnehmer angezeigt, aber die Optionen "Genehmigen", "Ablehnen" und "Neu zuweisen" sind nicht verfügbar. Änderungen, die sich aus Kampagnenentscheidungen ergeben, werden nicht mehr zu Bereitstellungsendpunkten exportiert.

Hinweis: Sie können einen Workflow nicht neu starten, nachdem Sie ihn angehalten haben.

Archivieren

Entfernt den Workflow aus allen Warteschlangen "Meine Aufgaben" und speichert den aktuellen Status des Workflow. Änderungen, die sich aus Kampagnenentscheidungen ergeben, werden nicht mehr zu Bereitstellungsendpunkten exportiert.

Eskalations-E-Mails

Ermöglicht es Ihnen, während einer Kampagne Erinnerungs-E-Mails zu definieren und zu senden (siehe Seite 66). Diese Funktion steht nur für Workflow-Kampagnen zur Verfügung.

Definieren und Senden von Eskalations-E-Mails

Administratoren können E-Mails senden, um Prüfer daran zu erinnern, ihre Aufgaben abzuschließen für eine Zertifizierungskampagne abzuschließen.

So definieren und senden Sie Eskalations-E-Mails

1. Wählen Sie im Fenster "Workflows" einen aktiven Workflow aus.

   Das Fenster "Workflow-Details" wird angezeigt.

2. Klicken Sie auf die Registerkarte "Verwaltung".
3. Klicken Sie auf "Eskalations-E-Mails"

   Das Popup "Eskalations-E-Mails" wird angezeigt.

   Hinweis: Die Eskalations-E-Mails-Schaltfläche wird nur für Zertifizierungskampagnen angezeigt.

4. Konfigurieren Sie die folgenden Informationen für jede E-Mail, die Sie senden wollen:
   - Abschlusskriterien
   - E-Mail-Vorlage
   - E-Mail-Empfänger
5. Um weitere E-Mails hinzuzufügen, klicken Sie auf das Plus-Symbol. Um E-Mails zu entfernen, klicken Sie auf die X-Symbole.

6. (Optional) Um E-Mail-Kriterien zu speichern, führen Sie die folgenden Schritte durch:

    a. Klicken Sie auf "Speichern".

       Das Popup "Kriterien der Eskalation speichern" wird angezeigt.

    b. Geben Sie einen Namen für das E-Mail-Kriterium an, und klicken Sie auf "Speichern".

       Die E-Mail-Kriterien werden gespeichert.

7. (Optional) Um E-Mail-Kriterien zu laden, führen Sie die folgenden Schritte durch:

    a. Klicken Sie auf "Laden".

       Das Popup "Kriterien der Eskalation laden" wird angezeigt.

    b. Wählen Sie eine Reihe von E-Mail-Kriterien aus, und klicken Sie auf "Laden".

       Die E-Mail-Kriterien werden geladen.

8. Klicken Sie auf "Jetzt senden".

   Eskalations-E-Mails werden an die Prüfer gesendet, deren Aufgaben dem Kriterium entsprechend abgeschlossen wurden.

Überwachung des Workflow-Fortschritts

Workflow-Eigentümer können den Fortschritt eines Workflow-Vorgangs, den sie über die Übersichtsregisterkarte in einem Workflow-Detailfenster eingeleitet haben, überwachen. Benutzer greifen auf die Übersichtsregisterkarte zu, indem sie "Verwaltung", "Workflows" öffnen und einen Workflow-Vorgang auswählen, um dessen Details anzuzeigen.

Die Übersichtsregisterkarte zeigt den Workflow-Fortschritt in Diagrammen an. Sie können den Fortschritt in jedem Diagramm als Prozentsatz oder als Wert anzeigen, indem Sie die entsprechende Option oberhalb eines jeden Diagramms auswählen. Wenn Sie "Wert" auswählen, zeigt CA RCM den Workflow-Fortschritt anhand der Anzahl von abgeschlossenen Aufgaben in diesem Workflow an.

Um das Diagramm zu aktualisieren, damit es den aktuellen Status wiedergibt, ohne dass die Übersichtsregisterkarte erneut geöffnet werden muss, klicken Sie auf "Diagramme erstellen".

Hinweis: Um zusätzliche Details über Aufgaben in einem Workflow-Fortschritt anzuzeigen, verwenden Sie die Registerkarten "Workflow-Fortschritt nach Prüfern" und "Workflow-Fortschritt nach betroffenen Entitäten" (siehe Seite 62).

Workflow-Fortschritt nach Entitäten oder Prüfern anzeigen

Das Fenster "Meine Anforderungen" und die "Workflows"-Fenster bieten zwei Methoden, den Fortschritt eines Workflow anzuzeigen.

- Die Registerkarte "Workflow-Fortschritt nach betroffenen Entitäten" gruppiert *Aufgaben* des Workflows nach den in Überprüfung befindlichen Entitäten einer jeden Aufgabe. Die Einträge in diesen Tabellen sind Aufgaben, die von CA RCM für den Workflow generiert wurden, und zwar basierend auf dem Workflowtyp, der Grundkonfiguration, des Umfangs der in Überprüfung befindlichen Entitäten und anderen Einstellungen.
- Die Registerkarte "Workflow-Fortschritt nach Prüfer" gruppiert *Aktionen des Workflows* zugewiesenen Prüfern und zeigt ihren Fortschritt. Die Einträge in diesen Tabellen sind Aktionen, die von den Workpoint-Jobs, die die Aufgaben des Workflows implementieren, generiert wurden.

Wenn ein Workflow in Bearbeitung ist, können Sie von jeder Registerkarte aus ein Drilldown durchführen, um individuelle Aktionen anzuzeigen. Die Registerkarte "Workflow-Fortschritt nach betroffenen Entitäten" zeigt von CA RCM erstellte High-Level-Aufgaben an. Die Hauptansichten dieser Registerkarte werden aufgefüllt, wenn CA RCM seine Analyse der in Überprüfung befindlichen Links im Workflow abschließt.

Jede dieser Aufgaben löst zahlreiche Workpoint-Jobs aus, wenn sie implementiert werden. Die Registerkarte "Workflow-Fortschritt nach Prüfer" zeigt die sich ergebenden Low-Level-Workpoint-Jobs an, sowie die Prüfer, die jedem Link zugewiesen wurden. Diese Registerkarte wird nur aufgefüllt, wenn Workpoint-Jobs initiiert werden, und ihr Inhalt hängt von der für jede Aufgabe durch den entsprechenden Workpoint-Prozess implementierten Logik ab.

Felder in Workflow-Fenstern

Verwenden Sie die folgenden Informationsfelder und interaktive Optionen, CA RCM-Workflow-Aktionen zu verarbeiten. Die für eine spezifische Aktion oder Gruppe von Aktionen verfügbaren Operationen hängen vom Typ einer jeden Aktion, dem zugewiesenen Prüfer und den Workflow- oder Systemeinstellungen ab.

Die folgenden Felder identifizieren den übergeordneten Workflow, der die Aktionen generierte:

Workflow-ID

Zeigt den eindeutigen numerischen Bezeichner an, den CA RCM jedem Workflow zuweist.

Workflow

Zeigt den Namen des Workflows an, der die Aktionen generierte.

Workflow-Beschreibung

Fahren Sie mit der Maus über das Symbol im Feld "Ablaufbeschreibung", um den Beschreibungstext des Workflows anzuzeigen, der die Aktionen generierte.

Workflow-Typ:

Zeigt den Namen des Workflows an, der die Aktionen generierte.

Initiator

Zeigt den Wert für das Feld "Personen-ID" des Benutzers an, der den Workflow initiierte.

Fälligkeitsdatum

Zeigt das Datum an, bis zu dem der Workflow-Initiator erwartet, dass Sie die Aktionen abschließen.

Die folgenden Felder und Operationen beziehen sich auf eine Gruppe von Aktionen im Übersichtsfenster "Meine Aufgaben", oder auf individuelle Aktionen:

Aktion

Zeigt den Aktionstyp (siehe Seite 45) für diese Aktion oder Gruppe von Aktionen an.

Benutzer/Rolle/Ressource

Identifiziert die primäre Entität, die allen Aktionen in einer Gruppe gemeinsam ist. Klicken Sie auf dieses Feld, um den Entitätsdatensatz für die Entität anzuzeigen.

Anwendername/Rollenname/Ressourcenname

Identifiziert die sekundäre Entität, die für jeden in Überprüfung befindlichen Link eindeutig ist. Beispiel: In einem Fenster mit Benutzerzertifizierungslinks zeigt diese Spalte Rollen und Ressourcen an, die mit dem sich in Überprüfung befindlichen Benutzer verknüpft sind. Klicken Sie auf dieses Feld, um den Entitätsdatensatz für die Entität anzuzeigen.

Fortschritt

Zeigt Ihren Fortschritt bei der Verarbeitung dieser Gruppe von Aktionen an.

Kommentar

Klicken Sie auf das Symbol in der Spalte "Kommentar", um einer Aktion oder Gruppe von Aktionen einen Kommentar hinzuzufügen (siehe Seite 55).

Anhang

Klicken Sie auf das Symbol in der Spalte "Anhang", um einer Aktion oder Gruppe von Aktionen eine Datei hinzuzufügen (siehe Seite 55).

Alert

Zeigt an, ob der Link bzw. die Gruppe von Links Auditkarten- oder Geschäftsprozessregeln verletzt. Der Wert in diesem Feld zeigt die Anzahl von Regeln an, die durch den Link verletzt werden. Klicken Sie auf den Wert, um eine detaillierte Liste von Verletzungen zu erhalten.

Aktions-ID

Zeigt den eindeutigen numerischen Bezeichner an, den CA RCM jeder Aktion zuweist.

Genehmigen

Klicken Sie auf das Symbol in der Spalte "Genehmigen", um einen Link zwischen der in Überprüfung befindlichen Entität und einer anderen Entität zu genehmigen.

Hinweis: Wenn die Gruppenauswahl für die Kampagne aktiviert ist, klicken Sie im Spaltenkopf auf das Kontrollkästchen "Genehmigen", um alle Links in einer Tabelle zu genehmigen.

Ablehnen

Klicken Sie auf das Symbol in der Spalte "Ablehnen", um einen Link zwischen der in Überprüfung befindlichen Entität und einer anderen Entität zu abzulehnen.

Hinweis: Wenn die Gruppenauswahl für die Kampagne aktiviert ist, klicken Sie im Spaltenkopf auf das Kontrollkästchen "Ablehnen", um alle Links in einer Tabelle zu abzulehnen.

Neu zuweisen

Klicken Sie auf das Symbol in der Spalte "Neu zuweisen", um eine Aktion auf einen anderen Prüfer zu übertragen (siehe Seite 53).

Hinweis: Wenn die Gruppenauswahl für die Kampagne aktiviert ist, klicken Sie im Spaltenkopf auf das Kontrollkästchen "Neu zuweisen", um alle Links in einer Tabelle zu neu zuzuweisen.

Ähnliche Informationen

Klicken Sie auf die Schaltfläche "Anzeigen", um andere Aktionen anzuzeigen, die mit dieser Aktion in Zusammenhang stehen, sowie zusätzliche Informationen, die für diese Aufgabe relevant sind.

Mitgliedschaft

Zeigt an, ob ein direkter Link, ein indirekter Link oder duale Links die in Überprüfung befindlichen Entitäten miteinander verbinden. Für vorgeschlagene Links hat dieses Feld den Wert "Nicht verknüpft".

Prüfer

Klicken Sie auf das Symbol in der Spalte "Prüfer", um eine Liste von anderen Prüfern für diese Verknüpfung anzuzeigen.

Auslastung

Zeigt die Auslastung aufgrund von Informationen von CA Enterprise Log Manager an.

Hinweis: Diese Informationen werden nur angezeigt, wenn CA RCM mit CA Enterprise Log Manager in Ihrer Umgebung integriert (siehe Seite 239) ist.

Konsultieren

Klicken Sie auf das Symbol in der Spalte "Konsultierung", um von anderen Prüfern Rat über eine Aktion zu erhalten.

Schließen

Entfernt eine Konsultierungsaktion aus der Warteschlange "Meine Aufgaben", ohne dem ursprünglichen Prüfer zu antworten. Dies bedeutet so viel, wie die Konsultierung abzulehnen. Kommentare oder Anhänge, die Sie dem in Überprüfung befindlichen Link hinzufügen, sind für die anderen Prüfer sichtbar.

Speichern

Speichert Ihre Überprüfungsentscheidungen und Ihre Neuzuweisungs-, Konsultierungs- und sonstigen Vorgänge, und kehrt zum Übersichtsfenster "Meine Aktionen" zurück. Diese Entscheidungen tragen zu Ihrem Fortschritt bei der Verarbeitung der Gruppe von Aktionen bei. Ihre Entscheidungen, Links zu genehmigen oder abzulehnen, werden noch nicht an CA RCM gesandt, und Sie können diese Entscheidungen überprüfen und ändern, wenn Sie sich das nächste Mal bei CA RCM anmelden.

Senden

Gibt CA RCM Ihre Entscheidungen weiter, Links zu genehmigen oder abzulehnen, und entfernt diese Aktionen aus Ihrem Fenster "Meine Aktionen".

Abbrechen

Verlässt das Detailfenster "Meine Aktionen", ohne Ihre Überprüfungsentscheidungen oder andere Vorgänge zu speichern.

Weitere Informationen:

Admin-Ansicht / Benutzeransicht (siehe Seite 201)

Kapitel 6: Ausführen von Zertifizierungskampagnen

Dieses Kapitel enthält folgende Themen:

Zertifizierungskampagnen

Zertifizierungskampagnen verwenden die Rollenhierarchie, Benutzerberechtigungen und Geschäftsregeln, die Sie in CA RCM zur Überprüfung angegeben haben. Wenn Sie eine Zertifizierungskampagne initiieren, werden Manager automatisch von CA RCM dazu aufgefordert, die Zugriffsrechte für von ihnen verwaltete Benutzer oder Ressourcen zu überprüfen. CA RCM bietet Ihnen Tools, um den Zertifizierungsprozess zu verfolgen, zu verwalten oder speziellen Bedürfnissen anzupassen, und die von Prüfern vorgeschlagenen Änderungen zu implementieren.

Zertifizierungskampagnen unterstützen folgende Geschäftsvorgänge:

- Bestätigung der Datensicherheit-Compliance – Falls gesetzlich vorgeschrieben wird, dass Maßnahmen zur Datensicherheit belegt werden müssen, werden Ihre regelmäßigen Überprüfungen der Datenzugriffe von Mitarbeitern in Zertifizierungskampagnen dokumentiert.
- Verfeinern der rollenbasierten Zugriffssteuerung – Durch die Überprüfung der Ressourcen und untergeordneten Rollen einer jeden Rolle kann bestätigt werden, dass die Rollenhierarchie dem derzeitigen Verwendungsmuster entspricht, und dass die Rollendefinitionen nützlich sind.

Verwenden des Dashboards

Sie können Zertifizierung-Workflows anpassen, um viele Geschäftsanforderungen zu unterstützen. Der grundlegende Kampagnenprozess sieht folgendermaßen aus:

1. Ein Rolleningenieur oder Administrator der oberen Ebene erstellt unter Berücksichtigung der gegebenen Geschäftsanforderungen die Kampagne in CA RCM. Der Kampagneneigentümer gibt die folgenden Informationen für die Kampagne an:

   - Das Universum, das die Grundlage für die Kampagne darstellt, sowie zusätzliche Daten wie Auditkarten und Mitgliederlisten, die in der Kampagne verwendet werden.
   - Filter, die den Umfang der Kampagne auf einen Teil der Entitäten oder Links in der Konfiguration beschränken.
   - So identifiziert die Kampagne Prüfer für jede Entitäts- und Berechtigungsverknüpfung
   - Umgang mit von Prüfern vollzogenen Änderungen.

   CA RCM erstellt die Kampagne und weist die überprüften Entitäten und Verknüpfungen automatisch an Manager und Administratoren zu.

2. Wenn die Kampagne startet, erhalten diese Manager über CA RCM eine Benachrichtigung per E-Mail, die einen Link zum CA RCM-Server enthält. Manager melden sich am CA RCM-Portal an, um die ihnen zugewiesenen Überprüfungsaktionen auszuführen.

3. Wenn Zertifizierer vorhandene Links ablehnen oder neue Links vorschlagen, muss die Konfigurationsdatei geändert werden. Über CA RCM werden die Manager der entsprechenden Entitäten benachrichtigt und um die Genehmigung der Änderung angefragt. Genehmigte Änderungen werden dann in der Zielkonfigurationsdatei implementiert.

Beispiel: Zertifizieren von Benutzerberechtigungen nach einem Erwerb

Der CA RCM-Konfiguration wurden nach einer Firmenerweiterung neue Benutzer und Ressourcen hinzugefügt. Administratoren führen eine Zertifizierungskampagne aus, um sicherzustellen, dass die Berechtigungen dieser neuen Benutzer angemessen sind.

Die Phasen der Kampagne lauten wie folgt:

1. Der Rolleningenieur erstellt eine Kampagne, die Benutzerentitäten und ihre Berechtigungs-Links zertifiziert. Der Rolleningenieur gibt Benutzerattributsfilter an, die den Umfang der Kampagne auf die neuen Mitarbeiter einschränken. Eine Mitgliederliste wird verwendet, um Manager zu den neuen Benutzern und Ressourcen zuzuordnen.

2. Jeder Manager überprüft die seinen Mitarbeitern zugewiesenen Berechtigungen. Bob Smith überprüft die Berechtigungen von Hector Torres, und schlägt vor, dass Hector Zugriff auf eine Datenbank erhält, die er in seiner neuen Position benötigt.

3. Über CA RCM erhält Deepak Chamarti, der Eigentümer der Datenbank, eine E-Mail. Deepak genehmigt die Änderung und CA RCM aktualisiert die Konfigurationsdatei. Hector Torres kann jetzt auf die Datenbank zugreifen.

Definieren und Starten von Kampagnen

Verwenden Sie den Assistenten zur Kampagnenerstellung wie nachfolgend beschrieben, um eine Kampagne zu erstellen, weisen Sie Datendateien zu und konfigurieren Sie Filter und andere Aspekte der Kampagne.

1. Planen Sie den Typ, Inhalt und Umfang sowie andere Funktionen der Kampagne (siehe Seite 88) entsprechend der Anforderungen Ihrer Geschäftsstrategie.

2. Überprüfen Sie, dass die in der Kampagne verwendeten Daten präzise und auf aktuellem Stand sind, und erstellen Sie zusätzliche für die Kampagne benötigte Dateien. Dazu zählen:

   - Auf der Modellkonfiguration des Universums basierende Konfigurationsdateien
   - Auditkarten, die Warnungen zu Verletzungen oder vorgeschlagene Links in der Kampagne enthalten
   - Mitgliederlisten und RACI-Konfigurations-Dateien, die Prüfer in der Kampagne zuordnen
   - Angepasste E-Mail-Vorlagen für die unterschiedlichen Meldungen, die CA RCM an Teilnehmer der Kampagne sendet

3. Gehen Sie im CA RCM-Portal zu "Verwaltung" und danach auf "Kampagne hinzufügen".

   Der Assistent zur Kampagnenerstellung wird angezeigt:

4. Geben Sie die folgenden Parameter der Kampagne im Fenster "Umfang" des Assistenten an:
   - Typ der zu erstellenden Kampagne
   - Zieluniversum
   - Auditkarten und andere Datensätze der Kampagne.
5. Geben Sie die folgenden Aspekte der Kampagne in dem Fenster Grundlegende Informationen (siehe Seite 79) des Assistenten an:
   - Name und kurze Beschreibung der Kampagne
   - Geschätzte Dauer der Kampagne
   - Anzeige von Auditkarten-Verletzungen (siehe Seite 111) in der Kampagne.
6. Geben Sie (siehe Seite 112) im Fenster "Filter" (siehe Seite 80) des Assistenten die Entitäten und Links an, die in der Kampagne enthalten sein sollen.
7. Geben Sie an, wie Links oder Entitäten ein zertifizierender Prüfer zugewiesen (siehe Seite 101) wird. Diese Einstellungen werden im Fenster "Prüfer" des Assistenten angezeigt. Sie können auch Prüfern erlauben, Gruppen von Entitäten zu zertifizieren bzw. festlegen, dass jede Entität einzeln überprüft und zertifiziert werden muss.
8. In diesem Fenster können Sie auch Prüfern erlauben, Überprüfungsentscheidungen auf Gruppen von Links oder Entitäten anzuwenden.

9. Geben Sie an, wie vorgeschlagene Änderungen der Konfiguration implementiert werden. Sie können die folgenden Funktionen konfigurieren:

   - Benutzerdefinierte Workflow-Vorgänge (siehe Seite 83) - jede Aufgabe der Kampagne wird mittels eines vordefinierten Prozesses implementiert. Wenn Administratoren alternative Prozessen definiert haben, können Sie angeben, welche Reihe von Prozessen die Ausführung von Kampagnenaufgaben steuert.

   - Fortlaufende Genehmigungen (siehe Seite 110): Sie können Genehmigungsaufgaben in einer zweiten Phase der Kampagne hinzufügen oder die Genehmigung/Änderung fortlaufend implementieren.

   - Ziel "Veränderungen implementieren"- wenn Sie eine Kampagne auf einer Konfigurationsdatei basieren, die nicht die Modellkonfiguration des Universums ist, können Sie Veränderungen aus der Kampagne in der Konfiguration, auf die verwiesen wird, oder in der Modellkonfiguration implementieren.

   Diese Einstellungen werden im Fenster "Ausführung" des Assistenten angezeigt.

10. Geben Sie an, wie CA RCM E-Mail an Kampagnenteilnehmer sendet, (siehe Seite 85) und welche E-Mail-Vorlagen verwendet werden. Diese Einstellungen werden im Fenster "Benachrichtigungen" des Assistenten angezeigt.

11. Das Fenster "Eigenschaften" des Assistenten zeigt optionale Kampagnenverhalten an. Die angezeigten Optionen hängen vom Kampagnentyp und von der Prozesszuordnung ab, die verwendet wird, um die Kampagne zu implementieren. Standardmäßig zeigt CA RCM die folgenden Optionsbereiche an:

    Benachrichtigungen

    CA RCM kann Änderungen, die sich aus der Kampagne ergeben, automatisch an die entsprechenden Bereitstellungsendpunkte exportieren. Wählen Sie die Option "Benachrichtigungen zu Modelländerungen für Export aktivieren" aus, um Änderungen an die Endpunkte zu exportieren.

    Genehmigungsverwaltung

    Wählen sie Optionen aus, die sich auf die Änderungsgenehmigungsüberprüfungsphase der Kampagne beziehen.

    - Genehmigungsprozess umgehen (siehe Seite 110): Sie können Änderungen direkt, ohne weitere Genehmigungen implementieren.
    - Unnötige Genehmigungen (siehe Seite 84) - Sie können unnötige Überprüfungsaktionen vermeiden, wenn der ursprüngliche Zertifizierer einer Entität auch Änderungen an der Entität überprüft.

    In diesem Fenster können Sie auch angeben, wie CA RCM Prüfer für Änderungen zuweist, die in der Überprüfung der Zertifizierung vorgeschlagen werden. Die folgenden Bereiche des Fensters lassen Sie angeben, wie Prüfer für jeden Typ von Entität ausgewählt werden:

    Auswahl von Prüfern von Ressourcenänderungen

    Geben Sie Prüferauswahlkriterien für Änderungen an Ressourcenentitäten an.

    Auswahl von Prüfern von Rollenänderungen

    Geben Sie Prüferauswahlkriterien für Änderungen an Ressourcenentitäten an.

    Auswahl von Prüfern von Benutzeränderungen

    Geben Sie Prüferauswahlkriterien für Änderungen an Ressourcenentitäten an.

12. Passen Sie das Tabellen-Layout in Aufgabentickets der Kampagne an.

13. Erstellen und starten Sie die Kampagne im Fenster "Zusammenfassung". Sie können die Kampagne sofort starten oder den Start zu einem späteren Zeitpunkt planen.

    Die Kampagne wird im Fenster "Workflows" im Verwaltungsmenü angezeigt.

    CA RCM generiert Überprüfungsaktionen basierend auf den Einstellungen der vorherigen Kampagne, verteilt sie auf die Warteschlangen "Meine Aufgaben" der teilnehmenden Prüfer und benachrichtigt diese Prüfer per E-Mail über die neuen Aktionselemente.

    CA RCM generiert auch Workflow-Steuerungsaktionen, die in der Warteschlange "Meine Aufgaben" des Kampagneninitiators erscheinen.

Fenster "Grundlegende Informationen"

Verwenden Sie dieses Fenster des Assistenten zur Kampagnenerstellung, um Namen, Beschreibung und andere Informationen für die Kampagne anzugeben. Folgende Felder sind nicht selbsterklärend:

Geschätzte Zeit

Gibt die geschätzte Dauer der Kampagne an. Nach diesem Zeitraum werden die Tickets der Kampagne als überfällig markiert, die Kampagne wird jedoch fortgesetzt.

Auditkartenwarnungen

Gibt an, ob Verletzungen einer Auditkarte in der Kampagne berücksichtigt werden sollen (siehe Seite 111). Es stehen unter anderem folgende Optionen zur Verfügung:

Keine

Kampagne enthält keinen Informationen der Auditkarte.

Von dieser Auditkarte

In Kampagnentickets werden zu überprüfende Links gekennzeichnet, die in der angegebenen Auditkarte angezeigt werden.

Eine Auditkarte für die Kampagne generieren

Während der Kampagneinitialisierung wird eine Auditkarte generiert, wobei die für das Zieluniversum angegebene Auditeinstellungsdatei verwendet wird. In Kampagnentickets werden zu überprüfende Links gekennzeichnet, die in dieser Auditkarte angezeigt werden.

Kommentare sind erforderlich, wenn Berechtigungen mit Verletzungen genehmigt werden

Wenn Prüfer einen Link mit Auditkarten-Verletzungen genehmigen, müssen sie einen Kommentar hinzufügen, der ihre Entscheidung, die Verknüpfung zu genehmigen, erklärt. Diese Option ist nur verfügbar, wenn Sie eine Auditkarte auf die Kampagne anwenden.

Fenster "Filter"

Verwenden Sie dieses Fenster, um den Umfang von Entitäten und Links, die in einer Zertifizierungskampagne enthalten sind, zu beschränken. Je nach Typ der erstellten Kampagne werden die folgenden Bereiche im Fenster angezeigt:

Benutzer/Rollen/Ressourcen auswählen

Definiert, welche Entitäten im Hinblick auf die Attributwerte in die Kampagne aufgenommen werden sollen.

Links

Gibt an, welche direkten, indirekten oder dualen Links in die Kampagne aufgenommen werden sollen.

Vorgeschlagene Links

Gibt an, ob CA RCM neue Links für Zertifizierer in dieser Kampagne vorschlagen soll, basierend auf Links in der Auditkarte, sowie welche vorgeschlagenen Links in die Kampagne aufgenommen werden.

Wenn Sie eine Auditkarte für die Kampagne angeben, werden die folgenden Felder angezeigt:

Filtern nach Auditkarte

Gibt an, wie Auditkartendaten verwendet werden, um die Links zu filtern, die in der Kampagne enthalten sind. Vorhandene Optionen:

Kein Auditkartenfilter

Auditkarten-Verletzungen werden nicht verwendet, um die Links der Kampagne zu filtern.

Einschließen, wenn in Auditkarte vorhanden

Die Kampagne enthält nur Links, die in der Auditkarte aufgelistet sind. In dieser Kampagne werden Links überprüft, die Geschäftsregeln verletzen.

Einschließen, wenn nicht in Auditkarte vorhanden

Die Kampagne enthält nur Links, die nicht in der Auditkarte aufgelistet sind.

Für differenzielle und Rezertifizierungskampagnen werden die folgenden Felder angezeigt:

Zustand auswählen

Gibt an, welche Links in einer Rezertifizierung oder differenziellen Kampagne enthalten sind, basierend auf ihrem letzten Zustand in der vorherigen Kampagne. Vorhandene Optionen:

Ausstehend

Enthält Links, die in der vorherigen Kampagne nicht überprüft wurden.

Genehmigt

Enthält Links, die in der vorherigen Kampagne genehmigt wurden.

Abgelehnt

Enthält Links, die in der vorherigen Kampagne abgelehnt wurden.

Wenn Sie die Option "Genehmigt" oder "Abgelehnt" auswählen, geben Sie eine der folgenden Optionen an, um festzulegen, wie die Entscheidungen der früheren Prüfer verarbeitet werden:

Auswahl der Genehmiger zurücksetzen

Berücksichtigt die Entscheidungen von früheren Prüfern in der aktuellen Kampagne nicht.

Auswahl der Genehmiger beibehalten

Zeigt die Entscheidungen von früheren Prüfern im Ticket der aktuellen Kampagne an. Prüfer können frühere Entscheidung aufheben. Dies ist die Standardeinstellung.

Links aktualisieren

Geben Sie an, ob Links, die nicht in der vorherigen Kampagne enthalten waren, aus der Konfiguration hinzugefügt werden sollen. Vorhandene Optionen:

Links hinzufügen, die nicht in der Quellkampagne enthalten sind

Neue und ausgeschlossene Links in der Konfiguration werden in dieser Kampagne berücksichtigt. Ein Symbol weist auf diese neuen Links in den Zertifizierungstickets der Kampagne hin.

Nicht aktualisieren

Diese Kampagne enthält nur Links, die in der vorherigen Kampagne enthalten waren.

Aktivierung der Gruppenüberprüfung von Aktionen

CA RCM-Administratoren können es Teilnehmern in einer Kampagne ermöglichen, Aktionen, die miteinander in Zusammenhang stehen, als Gruppe zu bearbeiten. Wenn die Gruppenbearbeitung aktiviert ist, zeigen die Fenster "Meine Aufgaben", die Kampagnenaktionen auflisten, Kontrollkästchen in den Spaltenköpfen "Genehmigen", "Ablehnen" und "Neu zuweisen". Prüfer überprüfen diese Kontrollkästchen, um eine Entscheidung für alle Links in der Tabelle zu treffen.

Um die Gruppenbearbeitung von zusammenhängenden Kampagnenaktionen zu aktivieren, aktivieren Sie im Fenster "Prüfer" des Assistenten "Kampagne hinzufügen" die Option "Ermöglichen Sie Managern, eine ganze Spalte auszuwählen".

Benutzerdefinierte Workflow-Vorgänge in einer Kampagne

CA RCM verwendet eine Reihe von vordefinierten Prozessen, um die Aufgaben einer Kampagne auszuführen. Administratoren können alternative Prozesse erstellen, die ändern, wie CA RCM Kampagnenaufgaben implementiert. Zum Beispiel können Administratoren eine Reihe von Prozessen definieren, für die höhere Verwaltungsebenen in Zertifizierungsüberprüfungen erforderlich sind. Wenn Sie eine Kampagne erstellen, können Sie angeben, welche Gruppe von Prozessen die Ausführung von Kampagnenaufgaben steuert.

Bevor Sie alternative Prozesse auf Ihre Kampagne anwenden können, müssen Administratoren die Prozesse erstellen, sie nach CA RCM importieren und sie zu Aufgaben des Kampagnen-Geschäfts-Workflows zuordnen.

Geben Sie die Prozesszuordnung für Ihre Kampagne im Fenster "Ausführung" des Assistenten zur Kampagnenerstellung an. Folgende Optionen stehen unter "Prozesse" zur Verfügung:

Systemstandardwerte

Verwendet die mit CA RCM installierten Standard-Workflow-Prozesse, um die Kampagne zu implementieren. Standardmäßiges Kampagnenverhalten wird ausgeführt.

Angepasste Prozesse

Verwendet die Prozesszuordnungsgruppe, die Sie in der Drop-down-Liste ausgewählt haben, um die Kampagne zu implementieren.

Prozesse

Zeigt die Prozesse an, die CA RCM aufruft, um die Hauptaufgaben der Kampagne basierend auf Ihrer Auswahl auszuführen.

Automatische Bearbeitung von unnötigen Überprüfungen

Oft nimmt der gleiche Prüfer sowohl an der vorbereitenden Zertifizierungsüberprüfung als auch an der nachfolgenden Änderungsgenehmigungsüberprüfung teil.

So ändert zum Beispiel während der Zertifizierungsüberprüfung ein Manager die Berechtigungen eines Mitarbeiters in seinem Team. Um diese Änderungen zu genehmigen, weist die Kampagne aufgrund der RACI-Konfiguration Prüfer zu, aber dieser Manager wird üblicherweise als der "Accountable"-Benutzer für den Mitarbeiter in der RACI-Konfiguration angegeben. Der für die Kampagne angegebenen Logik folgend, weist CA RCM die Änderungsgenehmigungsüberprüfung dem gleichen Manager zu, der die Änderung ursprünglich angefordert hat.

Standardmäßig geht CA RCM automatisch davon aus, dass der Prüfer die Änderung genehmigt, die während der Zertifizierung angefordert wurde. Wenn Sie eine Kampagne erstellen, können Sie die Prüfer zwingen, die Änderungen, die sie früher angefordert haben, zu erneut zu überprüfen.

Hinweis: Eine Überprüfungsaufgabe kann Beiträge von mehreren Prüfern erfordern. Diese Option bestimmt automatisch die Reaktion von früheren Prüfern - die Änderung wird nicht automatisch genehmigt.

Verwenden Sie die folgenden Optionen im Verwaltungsbereich "Genehmigen" Fensters "Eigenschaften"-, um dieses Verhalten zu steuern:

Anfrage an Prüfer zu Änderungen

Wenn sich aus der vorbereitenden Zertifizierungsüberprüfng neue oder gelöschte Links ergeben, initiiert CA RCM die Änderungsgenehmigungsüberprüfung, bevor es die Konfigurationsdatei ändert.

Der ursprüngliche Zertifizierer eines vorgeschlagenen Links genehmigt automatisch das Hinzufügen des Links.

Automatisch wird angenommen, dass Prüfer, die einen vorgeschlagenen Link während der vorbereitenden Zertifizierungsüberprüfung genehmigt haben, auch das Hinzufügen des Links zur Konfigurationsdatei genehmigen.

Der ursprüngliche Zertifizierer eines vorhandenen Links genehmigt automatisch Änderungen an dem Link.

Automatisch wird angenommen, dass Prüfer, die einen vorgeschlagenen Link während der vorbereitenden Zertifizierungsüberprüfung abgelehnt haben, seine Löschung aus der Konfigurationsdatei genehmigen.

Weitere Informationen:

Umgehen von Genehmigungsvorgängen für eine Kampagne (siehe Seite 110)

Definieren des E-Mail-Verhaltens für eine Kampagne

CA RCM verwendet eine Reihe vordefinierter Vorlagen, um auf die Kampagne bezogene E-Mail-Benachrichtigungen zu senden. Administratoren können alternative Vorlagen für einen oder mehrere E-Mail-Auslöser in Kampagnen erstellen. Wenn Sie eine Kampagne erstellen, können Sie angeben, welche Vorlage für jeden E-Mail-Auslöser der Kampagne verwendet werden sollte.

Bevor Sie alternative Vorlagen für Ihre Kampagne zuweisen können, müssen Administratoren die Vorlagen erstellen.

Sie geben die E-Mail-Vorlagen an, die in den Fenstern "Benachrichtigungen" des Assistenten zur Kampagnenerstellung verwendet werden sollen. Dieses Fenster listet E-Mail-Ereignisse auf, die für den Typ von Kampagne, die Sie erstellen, relevant sind.

Legen Sie das E-Mail-Verhalten für jedes E-Mail-Ereignis folgendermaßen fest:

1. Wählen Sie das Kästchen "Aktiv" neben einem E-Mail-Ereignis an, um E-Mail-Benachrichtigungen für dieses Ereignis zu aktivieren.
2. Wählen Sie für das Ereignis eine E-Mail-Vorlage aus der Vorlagen-Drop-down-Liste für das Ereignis aus.

Weitere Informationen:

Standard-E-Mail-Vorlagen (siehe Seite 232)
So passen Sie das E-Mail-Verhalten an (siehe Seite 227)

Anzeige von Kampagnenaktionen Anpassen

Sie können das Tabellen-Layout anpassen, das verwendet wird, um Kampagnenaktionen anzuzeigen.

Tabellen-Layouts für Workflow-Aktionen werden auf drei Ebenen definiert:

- Pro Universum: Administratoren definieren Standard-Tabellen-Layouts für alle auf dem Universum basierenden Workflows.
- Pro Kampagne: Kampagneninitiatoren können Tabellen-Layouts für die Aktionen einer Kampagne definieren. Benutzeranpassung auf dieser Ebene hat Vorrang gegenüber Universumsstandardwerten.
- Pro Benutzer: Benutzer können die Tabellen-Layouts in den Aktionsdetailsfenstern ihrer Warteschlange "Meine Aufgaben" anpassen. Benutzeranpassung auf dieser Ebene hat Vorrang gegenüber Kampagneneinstellungen oder Universumsstandardwerten.

Obligatorische Spalten können nicht aus Tabellenansichten entfernt werden. Roter Text und ein gesperrtes Schlosssymbol zeigen obligatorische Spalten in Benutzeranpassungsfenstern und Dialogfeldern an. Einige obligatorische Spalten sind hartkodierte Standards in CA RCM. Administratoren können zusätzliche obligatorischen Spalten definieren.

So passen Sie die Einstellungen für die Kampagnenanzeige an

1. Im Fenster "Zusammenfassung" des Assistenten zum Hinzufügen von Kampagnen öffnen Sie die Kopfzeile "Einstellungen anzeigen".

   Dieser Abschnitt enthält vier Tabellenköpfe. Die Kopfzeilen "Allgemeine Aktionen", "Benutzeraktionen", "Rollenaktionen" und "Ressourcenaktionen" zeigen die Tabellen-Layouts, die verwendet werden, um Aktionen in den Detailfenstern "Meine Aufgaben" anzuzeigen.

2. Passen Sie das Tabellen-Layout folgendermaßen an:

   a. Klicken Sie auf dem Tabellenkopf, den Sie ändern wollen, auf "Anpassen".

      Das Dialogfeld "Anpassen" wird angezeigt.

   b. Verwenden Sie die Pfeiltasten, um Spalten hinzuzufügen oder zu entfernen, und um die Spalten anzuordnen.

c. Wenn Sie die Spalten angepasst haben, klicken Sie auf OK.

d. Klicken Sie auf das Sperrsymbol neben dem Spaltennamen, um die Spalte obligatorisch zu machen. Benutzer können eine obligatorische Spalte verschieben, können sie jedoch nicht entfernen.

   Hinweis: Obligatorische Spalten werden in Rot angezeigt.

3. Klicken Sie auf "OK".

   CA RCM zeigt Aktionen für diese Kampagne in den Tabellenformaten an, die Sie angegeben haben.

Start-Optionen für Kampagnen

Sie können wählen, wann Sie eine Kampagne starten möchten. Die folgenden Startoptionen werden im letzten Zusammenfassungsfenster des Assistenten zur Kampagnenerstellung angezeigt:

Automatischer Start

Gibt an, wie die Kampagne gestartet wird. Vorhandene Optionen:

Manueller Start

CA RCM generiert die Kampagne, sendet jedoch keine Benachrichtigungen an die teilnehmenden Prüfer. Der Kampagneneigentümer startet die Kampagne von der Workflow-Steuerungsaktion in seiner Liste "Meine Aufgaben".

Sofortiger Start

CA RCM generiert die Kampagne und sendet Benachrichtigungen an die teilnehmenden Prüfer.

Geplanter Start

CA RCM generiert die Kampagne, sendet die Benachrichtigungen an die teilnehmenden Prüfer jedoch erst am geplanten Datum und zu einer festgelegten Zeit.

Hinweis: Wenn Sie den "Manueller Start" oder "Geplanter Start" auswählen, wird die Datenverarbeitung für die Kampagne sofort durchgeführt, und auf den aktuellen Inhalt der Konfiguration und anderer Datendateien bezogen.

Wenn Sie eine sich wiederholende Reihe von Kampagnen erstellen, sind nur der manuelle Start und der sofortige Start als Optionen verfügbar. Diese Optionen steuern den Start der ersten Kampagne in der Reihe. Verwenden Sie außerdem die folgenden Felder, um die periodische Wiederholung der Reihe zu definieren.

Erste Wiederholung

Definiert das Datum und die Uhrzeit, an dem CA RCM die zweite Kampagne in der Reihe initiiert.

Wiederholt sich alle

Definiert das Interval in Tagen zwischen Kampagnen in der Reihe.

Iterationen

Definiert die Anzahl von Kampagnen in der Reihe.

Kampagnentypen

Zertifizierungskampagnen unterstützen verschiedene Unternehmensanforderungen. CA RCM bietet die folgenden Arten an Zertifizierungskampagnen:

- Entitätenzertifizierung: Zertifizieren Sie die Links, die mit ausgewählten Benutzer-, Rollen- oder Ressourcen-Entitäten verknüpft sind.
- Rezertifizierung: Wiederholen Sie den auf eine frühere Kampagne basierten Zertifizierungsprozess.

Kampagnen zur Entitätenzertifizierung

Kampagnen zur Entitätenzertifizierung ermöglichen Prüfern, Links zwischen Benutzern, Rollen, und Ressourcen in einer CA RCM-Konfiguration zu überprüfen und zu zertifizieren.

Jede Kampagne zur Entitätenzertifizierung konzentriert sich auf eine Art von Entität und deren Links. Die folgenden Kampagnen sind möglich:

- In benutzerbezogenen Kampagnen werden Rollen und Ressourcen zertifiziert, die mit den einzelnen Benutzern verknüpft sind. Diese Links definieren die jedem Benutzer zugewiesenen Berechtigungen. Normalerweise überprüfen Manager die Berechtigungen ihrer Mitarbeiter.

  Verwenden Sie diesen Kampagnentyp, um die Compliance mit gesetzlich vorgeschriebenen Datensicherheitsmaßnahmen zu dokumentieren.

- In rollenbezogenen Kampagnen werden Ressourcen, übergeordnete oder untergeordnete Rollen und Benutzer zertifiziert, die mit den einzelnen Rollen verknüpft sind. Normalerweise überprüft der Rolleneigentümer die Links, die die Rolle definieren, sowie die Benutzer, die der Rolle zugewiesen wurden.

  Verwenden Sie diesen Kampagnentyp, um die Rollenhierarchie zu verwalten.

- In ressourcenbezogenen Kampagnen werden Benutzer und Rollen zertifiziert, die mit den einzelnen Ressourcen verknüpft sind. Normalerweise überprüft der Ressourcenadministrator die Rollen und Benutzer, die Zugriff zur Ressource haben.

  Verwenden Sie diesen Typ von Kampagne, um den Zugriff auf Ressourcen zu überwachen.

Um eine Kampagne zur Entitätenzertifizierung zu implementieren, wählen Sie die Option "Benutzerberechtigungen" oder "Ressourcenlinks" im Feld "Kampagnentyp" des Assistenten zur Kampagnenerstellung aus.

Selbstbewertungskampagnen

Eine Selbstbewertungskampagne ist eine Kampagne zur Benutzerzertifizierung, in der jeder zu prüfende Benutzer seine eigenen Berechtigungen zertifiziert.

Dieser Kampagnentyp entspricht einigen gesetzlichen Anforderungen bei der Datensicherheitszertifizierung. Dieser Kampagnentyp ist außerdem bei der Erstellung der Rollenhierarchie nützlich, und ist ein Ausgangspunkt für nachfolgende Zertifizierungen durch den Manager.

Wenn Sie Ihre Kampagne planen, überlegen Sie sich, wie Sie die Kampagnenergebnisse verwenden möchten. Normalerweise wird die aktive Konfiguration nicht durch die Selbstzertifizierung verändert. Wenn Sie eine Konfigurationsdatei erstellen möchten, die Benutzeränderungen widerspiegelt, nehmen Sie als Grundlage für die Kampagne eine Kopie der gewünschten Konfigurationsdatei.

Um eine Selbstbewertungskampagne zu implementieren, wählen Sie die Option "Selbstbewertung" im Feld "Kampagnentyp" des Assistenten zur Kampagnenerstellung aus. Der Assistent bietet Optionen, die mit diesem Kampagnentyp in Verbindung stehen:

- Weil jeder Benutzer sein eigener Prüfer ist, können Sie keine Prüfer basierend auf Mitgliederlisten oder einer RACI-Konfiguration zuweisen. Diese Optionen sind nicht verfügbar im Fenster "Prüfer" des Assistenten. Allerdings können Sie einen Standardprüfer für die Kampagne angeben.
- Standardmäßig werden Genehmigungs- und Implementierungsaufgaben in eine zweite, spätere Phase der Kampagne eingefasst, die Sie manuell starten müssen. Der Kampagneneigentümer erhält eine Workflow-Steuerungsaktion auf, die ihm erlaubt, die Genehmigungsphase zu initiieren.

Je nach Ihren Unternehmenszielen können Sie Informationen zur weiteren Verarbeitung aus der abgeschlossenen Kampagne als Auditkarte exportieren, oder Änderungen der Kampagne an der Zielkonfiguration implementieren. Sie können die Kampagne auch als die Grundlage für eine Rezertifizierung oder differenzielle Kampagne verwenden.

Rezertifizierungs-Kampagne

Mit einer Rezertifizierungs-Kampagne wird eine Reihe von Zertifizierungsaufgaben erstellt, die sich auf eine vorherige Kampagne beziehen.

Verwenden Sie diesen Kampagnentyp, wenn Sie mehrere Überprüfungen vornehmen möchten, bevor Änderungen implementiert werden. Zum Beispiel können Sie eine Kampagne zur Benutzerselbstbewertung erneut zertifizieren, in diesem Fall jedoch mit Managern anstelle von Mitarbeitern. Die Manager können im Laufe der Überprüfung die Ergebnisse der Benutzerselbstzertifizierung anzeigen.

Um eine Rezertifizierungs-Kampagne zu implementieren, wählen Sie die Option "Rezertifizierung" im Feld "Kampagnentyp" des Assistenten zur Kampagnenerstellung aus. Der Assistent bietet Optionen, die mit diesem Kampagnentyp in Verbindung stehen:

- Sie werden über den Assistenten aufgefordert, eine vorhandene Kampagne im Universum anzugeben. Die Rezertifizierungs-Kampagne bezieht sich auf diese frühere Kampagne.
- Weil die Basisaufgaben zur Überprüfung von der vorherigen Kampagne übernommen werden, können Sie die entsprechenden Links nicht nach Entitätsattributen filtern.

- Sie können jedoch angeben, welche direkten, indirekten oder dualen Links (siehe Seite 114) in die Kampagne aufgenommen werden sollen.
- Sie können enthaltene Links nach Endzustand der Überprüfungsaufgaben (siehe Seite 91) in der vorherigen Kampagne filtern.
- Wenn Sie möchten, können in CA RCM neue Links vorgeschlagen werden, basierend auf der für die Kampagne angegebenen Auditkarte.
- Sie können die Kampagne aktualisieren (siehe Seite 117), indem Sie Links zur Konfiguration hinzufügen, die in der vorherigen Kampagne nicht enthalten waren. Ein Symbol weist auf neue Links hin.
- Um Prüfer zuzuweisen. (siehe Seite 101), können Sie den Prüfer der vorherigen Kampagne oder den Manager des vorherigen Prüfers verwenden
- Standardmäßig werden Genehmigungs- und Implementierungsaufgaben in eine zweite, spätere Phase der Kampagne eingefasst, die Sie manuell starten müssen. Der Kampagneneigentümer erhält eine Workflow-Steuerungsaktion auf, die ihm erlaubt, die Genehmigungsphase zu initiieren.

Je nach Ihren Unternehmenszielen können Sie Informationen zur weiteren Verarbeitung aus der abgeschlossenen Kampagne als Auditkarte exportieren, oder Änderungen der Kampagne an der Zielkonfiguration implementieren. Sie können die Kampagne auch als die Grundlage für eine Rezertifizierung oder differenzielle Kampagne verwenden.

Zuvor überprüfte Links

Wenn Sie eine Rezertifizierungs-Kampagne erstellen, können Sie die in die neue Kampagne übernommenen Überprüfungsaufgaben nach dem Status in der alten Kampagne filtern. Wählen Sie im Fenster "Filter" des Assistenten zur Kampagnenerstellung eine der folgenden Optionen unter "Zustände" aus:

Ausstehend

Enthält Linkzertifizierungsaktionen, die nicht in der vorherigen Kampagne beschlossen wurden.

Genehmigt

Enthält Links, die in der vorherigen Kampagne genehmigt wurden.

Abgelehnt

Enthält Links, die in der vorherigen Kampagne abgelehnt wurden.

Hinweis: In Rezertifizierungskampagnen werden keine Kampagnensteuerungsaktionen aus der Referenzkampagne dupliziert. Nur Zertifizierungsaufgaben für Links oder Entitäten werden dupliziert.

Wenn Sie zuvor genehmigte oder abgelehnte Links einschließen, können Sie über die folgenden Optionen steuern, wie die Entscheidungen früherer Prüfer verarbeitet werden.

Auswahl der Genehmiger zurücksetzen

Frühere Überprüfungsentscheidungen werden nicht in die Rezertifizierungskampagne übernommen.

Auswahl der Genehmiger beibehalten

Auswahl des Genehmigers anzeigen

Prüfer der Rezertifizierungskampagne können frühere Überprüfungsentscheidungen anzeigen.

Die folgende Systemeigenschaft steuert, wie überprüfte Links früherer Prüfer in Rezertifizierungskampagnen präsentiert werden.

campaign.settings.recertification.allowOneClickResubmit

Legt fest, ob frühere Überprüfungsentscheidungen als aktive Optionen in Rezertifizierungsaufgaben präsentiert werden. Folgende Werte sind gültig:

Wahr

Vorherige Entscheidungen zur Genehmigung oder Ablehnung werden standardmäßig in Rezertifizierungsaufgaben ausgewählt. Prüfer in der Rezertifizierungskampagne können diese Entscheidungen annehmen, indem Sie im Fenster " Meine Aufgaben" auf "Senden" klicken. Der Assistent zur Kampagnenerstellung zeigt die Option "Auswahl der Genehmiger beibehalten" an.

Falsch

Vorherige Entscheidungen zur Genehmigung oder Ablehnung werden in Rezertifizierungsaufgaben durch grau hinterlegte Symbole angezeigt, diese Entscheidungen sind jedoch nicht standardmäßig ausgewählt. Prüfer in der Rezertifizierungskampagne müssen eine Überprüfungsentscheidung für jeden geprüften Link auswählen. Der Assistent zur Kampagnenerstellung zeigt die Option "Auswahl des Genehmigers anzeigen" an.

Differenzielle Kampagnen

Eine differenzielle Kampagne ist eine Rezertifizierungs-Kampagne, in der neue Links zertifiziert werden, die in der vorherigen Kampagne nicht enthalten waren und nun zur Konfiguration hinzugefügt wurden.

Um eine differenzielle Kampagne zu implementieren, wählen Sie die Option "Differenziell" im Feld "Kampagnentyp" des Assistenten zur Kampagnenerstellung aus. Der Assistent bietet Optionen zur Rezertifizierungs-Kampagne mit den nachfolgenden besonderen Einstellungen:

- Links der vorherigen Kampagne werden nicht berücksichtigt.
- Die Kampagne enthält nur Links, die der Konfiguration hinzugefügt wurden, nachdem die vorherige Kampagne erstellt worden war.

Je nach Ihren Unternehmenszielen können Sie Informationen zur weiteren Verarbeitung aus der abgeschlossenen Kampagne als Auditkarte exportieren, oder Änderungen der Kampagne an der Zielkonfiguration implementieren. Sie können die Kampagne auch als die Grundlage für eine Rezertifizierung oder differenzielle Kampagne verwenden.

Sich wiederholende Kampagne

Sie können eine Reihe von Rezertifizierungs-Kampagnen definieren, die sich in regelmäßigen Abständen wiederholen. Jede Kampagne in der Reihe basiert auf ihrer Vorgängerin.

Um eine sich wiederholende Kampagne zu implementieren, wählen Sie die Option "Rezertifizierung" im Feld "Kampagnentyp" des Assistenten zur Kampagnenerstellung aus. Der Assistent bietet Optionen, die mit diesem Kampagnentyp in Verbindung stehen:

- Sie können eine Benennungskonvention für Kampagnen in der Reihe angeben. Zeitstempel-Variablen in der Benennungskonvention geben jeder Kampagne in der Reihe einen eindeutigen Namen.
- Sie können die Zeitintervalle angeben, in denen CA RCM die Kampagnen der Reihe implementiert.
- Sie können alle optionalen Filter und Konfigurationen anwenden, die für Rezertifizierungskampagnen gültig sind. Zum Beispiel können Sie eine Reihe von differenzierenden Kampagnen erstellen, die nur neue Entitäten und Verknüpfungen zertifizieren.

Je nach Ihren Unternehmenszielen können Sie Informationen zur weiteren Verarbeitung aus der abgeschlossenen Kampagne als Auditkarte exportieren, oder Änderungen der Kampagne an der Zielkonfiguration implementieren. Sie können die Kampagne auch als die Grundlage für eine Rezertifizierung oder differenzielle Kampagne verwenden.

Namenskonventionen für sich wiederholende Kampagnen

Jede Kampagne muss eindeutige Werte für die Felder "Name" und "Beschreibung" haben.

Wenn Sie eine Reihe von sich wiederholenden Kampagnen erstellen, verwenden Sie Systemvariablen, um jeder Kampagne in der Reihe eindeutige Werte für Namen und Beschreibung zu geben. Normalerweise beruhen diese Felder auf der Quellkampagne für die Reihe. CA RCM ersetzt Systemvariablen durch eigentlichen Text und Datumswerte, wenn es eine Kampagne erstellt.

Verwenden Sie die folgenden Systemvariablen, um Zeichenfolgenwerte für die Felder "Name" und "Beschreibung" zu erstellen:

$sourceCampaignName

Fügt die Textzeichenfolge im Namensfeld der Quellkampagne für die Reihe ein.

$reoccurring

Fügt eine Zahl ein, die anzeigt, welche Iteration die genannte Kampagne in der Reihe ist.

$date

Fügt das Datum ein, an dem die genannte Kampagne erstellt wird.

$sourceCampaignDescription

Fügt die Textzeichenfolge im Beschreibungsfeld der Quellkampagne für die Reihe ein.

Beispiel: Namen sich wiederholender Kampagnen

Wenn Sie im Assistenten zur Kampagnenerstellung eine sich wiederholende Reihe erstellen, wird das Namensfeld im Fenster "Grundlegende Informationen" automatisch anhand der folgenden Formel aufgefüllt:

```
$sourceCampaignName Recurring # $reoccurring @ $date
```

Wenn die Quellkampagne "UserCert" benannt wird und die Reihe sich täglich wiederholt, werden die ersten drei Kampagnen in der Reihe folgendermaßen benannt:

```
UserCert Recurring # 1 @ 12Nov2010
UserCert Recurring # 2 @ 13Nov2010
UserCert Recurring # 3 @ 14Nov2010
```

Mögliche Aktionen während einer Kampagne

Während einer aktiven Kampagne kann der Administrator die folgenden Aktionen ausführen:

- Überprüfen und zertifizieren von direkt zugewiesenen Links
- Neu zuweisen von Überprüfungsaufgaben
- Anhängen von Kommentaren, Dateien oder Links an eine Gruppe von Aufgaben
- Überwachen des Kampagnenfortschritts

- Senden von Eskalations-E-Mails an teilnehmende Prüfer
- Abbrechen und Neu starten der Kampagne
- Speichern von Entscheidungen zu Zertifizierungen (siehe Seite 98) in einer Auditkarte
- Initiieren der Genehmigungs- und Implementierungsphase der Kampagne

Ein Zertifizierungs-Prüfer kann die folgenden Aktionen ausführen:

- Überprüfen und zertifizieren von direkt zugewiesenen Links
- Neu zuweisen von Überprüfungsaufgaben
- Anhängen von Kommentaren, Dateien oder Links an eine Aufgabe oder eine Gruppe von Aufgaben

Weitere Informationen:

Initiieren der Genehmigungsphase einer Kampagne (siehe Seite 96)
Wiederverwendung von Entscheidungen zu Zertifizierungen (siehe Seite 98)

Initiieren der Genehmigungsphase einer Kampagne

Standardmäßig werden Zertifizierungskampagnen in Zertifizierungs- und Änderungsgenehmigungsphasen eingeteilt (siehe Seite 100). Der Kampagneninitiator oder CA RCM-Administrator beendet manuell die Zertifizierungsphase und initiiert die Änderungsgenehmigungsphase.

Wenn Sie fortlaufende Genehmigungen für die Kampagne konfiguriert haben, werden Überprüfungs- und Genehmigungsaufgaben nicht in unterschiedliche Phasen aufgeteilt, und Sie brauchen Änderungsgenehmigungen nicht manuell einzuleiten.

Wichtig! Wenn Sie die Genehmigungsphase initiieren, werden alle unvollständigen Zertifizierungsaufgaben abgebrochen. Dies kann sich auf die Vollständigkeit der Zertifizierungskampagne und die Nutzbarkeit seiner Ergebnisse auswirken. Verwenden Sie die Workflow-Administrationsschnittstelle, um den Fortschritt der Kampagne zu überprüfen, bevor Sie die Genehmigung von Änderungen initiieren.

So initiieren Sie die Genehmigungsphase einer Kampagne

1. Öffnen Sie die Workflow-Steuerungsaktion für die Kampagne:
   - Kampagneneigentümer: Klicken Sie In ihrer Warteschlange "Meine Aufgaben" auf die Aktion, die sich auf die Kampagne bezieht, die in der Tabelle "Allgemeine Aufgaben" angezeigt wird.
   - Administratoren: Klicken Sie im Fenster "Workflow-Verwaltungs" auf die Registerkarte "Fortschritt des Ablaufs nach Prüfern" und wenden Sie den Aktionstypfilter "Andere" an, um die Workflow-Steuerungsaktion zu finden.

   Die angezeigte Aktion hat das folgende Benachrichtigungsfeld:

   ```
   Klicken Sie auf "Genehmigungen starten", um die Kampagnenzertifizierung
   anzuhalten und mit dem Genehmigungsprozess fortzufahren.
   ```
2. (Optional) Klicken Sie auf "Neu zuweisen", um die Steuerung der Kampagne an einen anderen Benutzer zu übertragen.
3. Klicken Sie in der Spalte "Zugehörige Informationen", auf "Anzeigen", um den Kampagnenfortschritt zu überprüfen. Stellen Sie sicher, dass Zertifizierungsaufgaben für Ihre Geschäftsziele genügend fortgeschritten sind.
4. Wählen Sie in der Spalte "Benutzerdefiniert" die Option "Genehmigungen starten" aus.
5. Klicken Sie auf "Senden".

   CA RCM bricht Zertifizierungsaktionen ab, die noch nicht abgeschlossen sind, und entfernt sie aus der Warteschlange "Meine Aufgaben" der teilnehmenden Prüfer.

   CA RCM initiiert Genehmigungsüberprüfungen für Änderungen an Entitäten oder Links, die während der ursprünglichen Zertifizierung angefragt wurden.

Wiederverwendung von Entscheidungen zu Zertifizierungen

Sie können die Entscheidungen von Zertifizierern in einer Kampagne in einer Datendatei speichern. Diese Daten können die Grundlage für zusätzliche Kampagnen oder analytische Prozesse bilden.

Die Datendatei ist eine Variante des standardmäßigen Auditkartenformats. Diese Auditkarte zeichnet die Ergebnisse der anfänglichen Zertifizierungsüberprüfung auf. Die Auditkarte filtert diese auf die letzte Genehmigungsphase der Kampagne basierten Entscheidungen *nicht*. Alle Entscheidungen zu Zertifizierungen werden gespeichert, auch wenn die Ressourceneigentümer oder -Manager die angeforderten Änderungen nicht genehmigt haben.

Speichern von Entscheidungen zu Zertifizierungen in einer Auditkarte

Sie können die Entscheidungen von Zertifizierern in einer Kampagne in einer Datendatei speichern. Diese Daten können die Grundlage für zusätzliche Kampagnen oder analytische Prozesse bilden.

So speichern Sie Entscheidungen zu Zertifizierungen in einer Auditkarte

1. Gehen Sie im CA RCM-Portal zu "Verwaltung" und danach auf "Kampagnenverwaltung".

   Das Fenster "Kampagnenverwaltung" wird angezeigt.

2. Klicken Sie auf "Fortschritt der Kampagne in Auditkarte exportieren".

   Hinweis: Um aus einer Kampagne, die mit CA RCM Version 3.2 erstellt wurde, zu exportieren, klicken Sie auf "V3.2-Kampagne in die Auditkarte exportieren".

   Das Fenster "Fortschritt der Kampagne in Auditkarte exportieren" wird angezeigt.

3. Wählen Sie eine aktive Kampagne aus, geben Sie den Namen der Auditkarte ein, die die gespeicherten Daten enthält.

   Hinweis: Wenn Sie eine vorhandene Auditkarte angeben, werden die Daten der Auditkarte überschrieben.

4. Klicken Sie auf "Exportieren".

   Eine Auditkarte wird erstellt, die die ursprüngliche Zertifizierungsphase der von Ihnen angegebenen Kampagne aufzeichnet. Die Auditkarte enthält *keine* Entscheidungen der letzten Genehmigungsphase der Kampagne.

Importieren von Entscheidungen zu Zertifizierungen in eine Kampagne

Sie können die von Zertifizierern in einer früheren Kampagne getroffenen Entscheidungen in eine neue Kampagne importieren.

So importieren Sie Entscheidungen zu Zertifizierungen in eine Kampagne

1. Erstellen Sie eine Kampagne. Wählen Sie im Fenster "Zusammenfassung" des Assistenten zur Kampagnenerstellung die Option "Deaktiviert" im Feld "Automatischer Start".

   Die Kampagne wird in CA RCM generiert, startet jedoch nicht.

2. Gehen Sie im CA RCM-Portal zu "Verwaltung" und danach auf "Kampagnenverwaltung".

   Das Fenster "Kampagnenverwaltung" wird angezeigt.

3. Klicken Sie auf "Fortschritt der Zertifizierung von Auditkarte importieren".

   Das Fenster "Fortschritt der Zertifizierung von Auditkarte importieren" wird angezeigt.

4. Geben Sie die inaktive Kampagne sowie die Auditkarte an, die die gespeicherten Daten enthält.

5. (Optional) Wählen Sie die Option "Unveränderte Aufgaben löschen", um Entitäten und Links zu löschen, denen keine Entscheidungen in der Auditkarte der Kampagne entsprechen.

   Die Kampagne enthält nur Entscheidungen, die in der Auditkarte angezeigt werden.

   Hinweis: Um diese Option effektiv zu verwenden, erstellen Sie eine Kampagne die dem Umfang und den Einstellungen der ursprünglichen Kampagne ähnlich ist.

6. Klicken Sie auf "Importieren".

   Entscheidungen zu Überprüfungen in der Auditkarte, die sich auf Entitäten und Links in der Kampagne beziehen, werden in die Kampagne kopiert.

7. Gehen Sie zu ihrer Liste "Mein Aufgaben", um die Kampagne zu starten.

Zertifizierungs- und Genehmigungsstufen einer Kampagne

Die meisten Zertifizierungskampagnen bestehen aus zwei Phasen:

- **Zertifizierung**: Manager und Ressourceneigentümer prüfen die Links der Benutzer, Rollen und Ressourcen, die sie verwalten. Ein Manager überprüft zum Beispiel die Berechtigungen seiner Mitarbeiter bzw. ein Rolleneigentümer überprüft die Ressourcen, die in einer Rolle enthalten sind.
- **Genehmigung**: Wenn ein Link in der Prüfphase abgelehnt wird oder ein neuer Link vorgeschlagen wird, muss der Manager der verknüpften Ressource die vorgeschlagenen Änderungen genehmigen. Wenn zum Beispiel der Manager den Zugriff eines seiner Mitarbeiter auf eine bestimmte Ressource ablehnt, muss der Eigentümer dieser Ressource diese Änderung bestätigen. Nur abgelehnte Links oder neue Links lösen eine Genehmigungsaufgabe aus, da sie die Basiskonfiguration ändern.

Standardmäßig haben Kampagnen unterschiedliche Überprüfungs- und Genehmigungsphasen. Genehmigungsaufgaben werden zurückgestellt, bis alle Zertifizierungsaufgaben vollständig sind. Der Kampagneneigentümer initiiert die Genehmigungsphase vom Stammticket der Kampagne aus. Genehmigungsaufgaben und Benachrichtigungen werden konsolidiert, wodurch die Arbeit der Ressourceneigentümer erleichtert wird.

Sie können die Kampagne so konfigurieren, dass Genehmigungsaufgaben sofort initiiert werden, wenn ein Prüfer einen abgelehnten Link sendet. Die Prüf- und Genehmigungsphasen der Kampagne überschneiden sich. Sowohl die Prüfphase als auch die Genehmigungsphase sind großteils während der Kampagne aktiv. Diese Kampagnestruktur hat einige Nachteile, besonders für Kampagnen mit großem Umfang. Da Genehmigungsaufgaben nicht konsolidiert werden, bekommen Ressourceneigentümer und -Manager eine separate E-Mail-Benachrichtigung für jede Änderung, die sie genehmigen sollen. Die Genehmigungsphase wird erweitert, und die Anzahl an Benachrichtigungen und Genehmigungsaufgaben kann ablenken und ist möglicherweise unkontrollierbar. Ressourceneigentümer können die Gesamtauswirkung von aus der Kampagne resultierenden Änderungen nicht abschätzen.

So weist CA RCM Zertifizierer zu

In CA RCM werden die Entitätsattribute analysiert, um einen Manager oder Ressourceneigentümer für die einzelnen zu überprüfenden Entitäten oder Links zu lokalisieren.

In Kampagnen zur Entitätenzertifizierung können Sie mithilfe von CA RCM Prüfer folgendermaßen zuweisen:

- Suchen Sie in einer vordefinierten Mitgliederliste am Server nach einem auf die Entität bezogenen Benutzer.
- Suchen Sie in der RACI-Konfiguration des Universums nach einem Benutzer, der Accountable oder Responsible für die Entität ist.

  Hinweis: Für Kampagnen zur Benutzerzertifizierung wird in CA RCM zuerst das Feld des Benutzermanagers der Konfiguration im Zieluniversum nach dem Manager der einzelnen Benutzer abgefragt.
- Weisen Sie die Aufgabe einem für die Kampagne angegebenen Standardprüfer zu.
- Lassen Sie Benutzer ihre eigenen Links genehmigen. Diese Option bezieht sich nur auf Kampagnen zur Selbstbewertung.

Bei Rezertifizierungen und differenziellen Kampagnen können Sie mithilfe von CA RCM Prüfer folgendermaßen zuweisen:

- Suchen Sie in einer vordefinierten Mitgliederliste am Server nach einem auf die Entität bezogenen Benutzer.
- Durchsuchen Sie die RACI-Konfiguration des Universums nach Folgendem:
  - Benutzer, der "Accountable" oder "Responsible" für die Entität in der aktuellen Konfiguration ist.
  - Prüfer, der in der vorherigen Kampagne zugewiesen wurde.
  - Manager des vorherigen Prüfers, basierend auf dem für das Zieluniversum angegebene Feld des Benutzermanagers der Konfiguration.
- Weisen Sie die Aufgabe einem für die Kampagne angegebenen Standardprüfer zu.

Wenn Sie eine Kampagne erstellen, können Sie angeben, welches dieser Verfahren CA RCM zur Lokalisierung eines Zertifizierers verwendet soll, und in welcher Reihenfolge die Verfahren verwendet werden.

Beispiel: Zuweisen eines Prüfers

Die folgenden Schritte beschreiben, wie ein Prüfer für eine Kampagne gefunden werden kann:

1. Zuerst soll CA RCM eine Mitgliederliste konsultieren. Wird ein Prüfer in der Mitgliederliste festgestellt, wird der Prozess beendet.
2. Wenn kein Prüfer in der Mitgliederliste festgestellt wird, konsultiert CA RCM anschließend die RACI-Konfiguration. Wird ein Prüfer festgestellt, wird der Prozess beendet.
3. Wenn kein Prüfer in der RACI-Konfiguration festgestellt wird, wird die Zertifizierungsaufgabe einem Standardprüfer zugewiesen.

Mitgliederlisten

Eine Mitgliederliste ist ein Datensatz, der Benutzernamen und Attribute enthält. Sie können Mitgliederlisten verwenden, um Prüfer in einer Zertifizierungskampagne zuzuweisen.

Jeder Eintrag der Mitgliederliste enthält die folgenden drei Felder:

Anmeldung

Gibt ein Benutzerkonto in CA RCM an. Dieses Feld hat denselben Inhalt und dasselbe Format wie das Feld "Anmelde-ID" einer Benutzer- oder Konfigurationsdatei.

Kategorie

Gibt ein Benutzer-, Rollen- oder Ressourcenattribut an. Dieses Feld kann unterschiedliche Werte für jeden Datensatz in der Mitgliederliste haben. Um mit Entitäten in der Kampagne übereinzustimmen, geben Sie Attribute an, die in der Konfigurationsdatei, auf die sich die Kampagne bezieht, vorhanden sind.

Wert

Gibt den Wert des im Feld "Kategorie" aufgelisteten Attributs an.

Um einen Prüfer für eine Entität zuzuweisen, durchsucht CA RCM die Mitgliederliste und vergleicht Attributwerte der Mitgliederliste mit den Attributwerten der Entität. CA RCM weist Überprüfungsaufgaben für die Entität jenem Benutzer zu, der als *erster* Datensatz in der Mitgliederliste mit einem Attributwert der Entität übereinstimmt.

Hinweis: Eine Mitgliederliste kann nur Attribute für einen Entitätstypen enthalten: Benutzer, Rolle oder Ressource. Allerdings kann eine Mitgliederliste Attribute und Werte aus unterschiedlichen Universen enthalten. Nur das Feld "Anmelde-ID" muss einheitlich in allen Universen angegeben werden, die mit der Mitgliederliste verwendet werden.

Sie können Mitgliederlistendateien in CA RCM importieren oder Administratorfenster des Portals verwenden, um Mitgliederlisten zu erstellen und zu bearbeiten.

Beispiel: Prüfer mit Ressourcenattributen übereinstimmen

Die folgende Mitgliederliste verknüpft Benutzer mit verschiedenen Ressourcenattributwerten:

Anmeldung	Kategorie	Wert
DOMAIN\Hector_Torres	ResName3	Solaris
DOMAIN\Anna_Chiu	Standort	Atlanta
DOMAIN\Alex_Patrick	ResName3	WinNT
DOMAIN\Kim_Bell	Organisation	Marketing – Sun-Server

Diese Mitgliederliste wird zur Zuweisung von Prüfern in einer Kampagne zur Ressourcenzertifizierung verwendet. Die folgenden Ressourcen werden überprüft:

- Die Ressource "Domain_Users" mit den folgenden Attributwerten:

  ResName3 = Solaris

  Standort = Atlanta

  CA RCM verwendet den *ersten* übereinstimmenden Datensatz in der Liste, und weist Hector Torres als Überprüfer der Links in dieser Ressource zu.

- Die Ressource "Einkauf" mit den folgenden Attributwerten:

  Organisation = Hauptquartier

  Keine Datensätze in der Mitgliederliste stimmen mit dieser Entität überein. CA RCM kann mit den Daten der Mitgliederliste keinen Prüfer zuweisen.

Weitere Informationen:

Erstellen von Mitgliederlisten (siehe Seite 104)
Erstellen von Mitgliederlisten aus CSV-Dateien (siehe Seite 105)
Klonen von Mitgliederlisten (siehe Seite 106)
Bearbeiten von Mitgliederlisten (siehe Seite 107)
Sonderzeichen für Mitgliederlisten (siehe Seite 109)

Erstellen von Mitgliederlisten

Sie können Mitgliederlisten verwenden, um Prüfer für eine Kampagne zuzuweisen. Sie haben mehrere Möglichkeiten, um eine Mitgliederliste zu erstellen: Verwenden Sie diesen Vorgang, um eine Mitgliederliste interaktiv im CA RCM-Portal zu erstellen.

So erstellen Sie Mitgliederlisten

1. Im Hauptmenü des CA RCM-Portals klicken Sie auf "Verwaltung", "Workflow-Einstellungen" und "Mitgliederlisten verwalten".

   Das Fenster "Mitgliederliste" wird angezeigt.

2. Geben Sie im Bereich "Mitgliederliste hinzufügen" eine neue Mitgliederliste an. Das folgende Feld ist nicht selbsterklärend:

   Kampagnentyp

   Gibt den Typ der Kampagne an, die die Mitgliederliste verwendet. Zum Beispiel funktioniert eine Mitgliederliste, die Rollenattribute enthält, mit einer Kampagne zur Rollenzertifizierung.

3. Deaktivieren Sie die Option "CSV-Datei verwenden".
4. Klicken Sie auf "Hinzufügen".

   Das Fenster "Mitgliederliste bearbeiten" wird angezeigt.
5. Verwenden Sie die Optionen "Hinzufügen", "Bearbeiten" und "Löschen" (siehe Seite 107), um die Mitgliederliste zu bearbeiten.
6. Klicken Sie auf "Speichern".

   Die Änderungen wurden in der Mitgliederliste gespeichert. Das Hauptfenster "Mitgliederlistenverwaltung" wird angezeigt. Die neue Liste wird in der Tabelle der Mitgliederlisten angezeigt.

Weitere Informationen:

Erstellen von Mitgliederlisten aus CSV-Dateien (siehe Seite 105)
Klonen von Mitgliederlisten (siehe Seite 106)
Bearbeiten von Mitgliederlisten (siehe Seite 107)
Sonderzeichen für Mitgliederlisten (siehe Seite 109)

Erstellen von Mitgliederlisten aus CSV-Dateien

Sie können Mitgliederlisten verwenden, um Prüfer für eine Kampagne zuzuweisen. Sie haben mehrere Möglichkeiten, um eine Mitgliederliste zu erstellen: Verwenden Sie diesen Vorgang, um eine Mitgliederliste zu erstellen, die sich auf eine importierte Datei mit kommagetrennten Werten basiert.

So erstellen Sie Mitgliederlisten aus CSV-Dateien

1. Bereiten Sie die Datendatei vor. Die erste Zeile der CSV-Datei muss wie folgt lauten:

   ```
   anmeldung,kategorie,wert
   ```

   Hinweis: Verwenden Sie nur Kleinbuchstaben in dieser Kopfzeile.

   Jede Zeile der Datei muss drei Werte enthalten, die durch Kommas getrennt sind. Das folgende Beispiel zeigt eine CSV-Datei mit zwei Datensätzen:

   ```
   anmeldung,kategorie,wert
   DOMAIN\Alex_Patrick,ResName3,WinNT
   DOMAIN\Kim_Bell,Organisation,Marketing – Sun-Server
   ```
2. Im Hauptmenü des CA RCM-Portals klicken Sie auf "Verwaltung", "Workflow-Einstellungen" und "Mitgliederlisten verwalten".

   Das Fenster "Mitgliederliste" wird angezeigt.

3. Geben Sie im Bereich "Mitgliederliste hinzufügen" eine neue Mitgliederliste an. Das folgende Feld ist nicht selbsterklärend:

   Kampagnentyp

   Gibt den Typ der Kampagne an, die die Mitgliederliste verwendet. Zum Beispiel funktioniert eine Mitgliederliste, die Rollenattribute enthält, mit einer Kampagne zur Rollenzertifizierung.

4. Klicken Sie auf die Option "CSV-Datei verwenden" und suchen Sie die vorbereitete CSV-Datei.
5. Klicken Sie auf "Hinzufügen".

   CA RCM erstellt eine auf die CSV-Datei basierende Mitgliederlistendatei. Die Mitgliederliste wird in der CA RCM-Datenbank gespeichert, und die neue Datei wird in der Liste von Mitgliederlisten angezeigt.

6. (Optional) Klicken Sie neben der neuen Datei auf "Bearbeiten", um den Inhalt zu überprüfen bzw. zu bearbeiten.

Klonen von Mitgliederlisten

Sie können Mitgliederlisten verwenden, um Prüfer für eine Kampagne zuzuweisen. Sie haben mehrere Möglichkeiten, um eine Mitgliederliste zu erstellen: Verwenden Sie diesen Vorgang, um eine Mitgliederliste zu erstellen, die sich auf die Kopie einer vorhandenen Mitgliederliste bezieht.

So klonen Sie Mitgliederlisten

1. Im Hauptmenü des CA RCM-Portals klicken Sie auf "Verwaltung", "Workflow-Einstellungen" und "Mitgliederlisten verwalten".

   Das Fenster "Mitgliederliste" wird angezeigt. In einer Tabelle werden die Mitgliederlisten der CA RCM-Datenbank aufgelistet.

2. Klicken Sie auf das Symbol "Kopieren" der Mitgliederliste, die Sie kopieren wollen.

   Das Fenster "Mitgliederliste kopieren" wird angezeigt.

3. Geben Sie einen neuen Namen für die Mitgliederliste an, und klicken Sie auf "OK".

   Hinweis: Sie können diesen Namen nicht mehr bearbeiten, nachdem die Liste erstellt wurde.

   Eine neue Mitgliederliste wird in der Tabelle mit dem von Ihnen angegebenen Namen angezeigt. Die Liste enthält die gleichen Datensätze wie die Basisliste.

4. Klicken Sie auf das Symbol "Bearbeiten" der neuen Liste.

   Das Fenster "Mitgliederliste bearbeiten" wird angezeigt.

5. Verwenden Sie die Optionen "Hinzufügen", "Bearbeiten" und "Löschen" (siehe Seite 107), um die Mitgliederliste abzuändern.

6. Klicken Sie auf "Speichern".

   Die Änderungen wurden in der Mitgliederliste gespeichert. Das Hauptfenster "Mitgliederlistenverwaltung" wird angezeigt.

Bearbeiten von Mitgliederlisten

Sie können Mitgliederlisten verwenden, um Prüfer für eine Kampagne zuzuweisen. Verwenden Sie diesen allgemeinen Vorgang, um eine Mitgliederliste im CA RCM-Portal zu bearbeiten.

So bearbeiten Sie Mitgliederlisten

1. Im Hauptmenü des CA RCM-Portals klicken Sie auf "Verwaltung", "Workflow-Einstellungen" und "Mitgliederlisten verwalten".

   Das Fenster "Mitgliederliste" wird angezeigt. In einer Tabelle werden die Mitgliederlisten der CA RCM-Datenbank aufgelistet.

2. Klicken Sie auf das Symbol "Bearbeiten" der Mitgliederliste, die Sie bearbeiten wollen.

   Das Fenster "Mitgliederliste bearbeiten" wird angezeigt.

3. Fügen Sie der Mitgliederliste neue Datensätze folgendermaßen hinzu:

   a. Wählen Sie die Konfigurationsdatei aus, auf die sich dieser Datensatz bezieht. Die Dropdown-Liste zeigt verfügbare Konfigurationen an.

   b. Klicken Sie auf "Hinzufügen".

      Das Popup "Eintrag hinzufügen" wird angezeigt.

   c. Wählen Sie Benutzer, Attributfeld und Wert aus. Es sind nur Werte der Basiskonfiguration verfügbar.

   d. Klicken Sie auf "OK".

      Der Datensatz wurde der Mitgliederliste hinzugefügt, und wird in der Tabelle angezeigt.

4. Bearbeiten Sie Datensätze in der Mitgliederliste folgendermaßen:

   a. Suchen Sie den Datensatz in der Tabelle und klicken Sie auf das Symbol "Bearbeiten" des Datensatzes.

      Das Popup "Bearbeiten" wird angezeigt.

   b. Wählen Sie Benutzer, Attributfeld und Wert aus. Es sind nur Werte der Basiskonfiguration dieses Datensatzes verfügbar.

   c. Klicken Sie auf "OK".

      Der Datensatz wurde aktualisiert. Neue Werte für diesen Datensatz werden in der Tabelle angezeigt.

5. Um einen Datensatz zu löschen, suchen Sie den Datensatz in der Tabelle, und zu klicken Sie auf das Symbol "Löschen" des Datensatzes.

   Der Datensatz wurde aus der Mitgliederliste gelöscht.

6. Klicken Sie auf "Speichern".

   Die Änderungen wurden in der Mitgliederliste gespeichert. Das Hauptfenster "Mitgliederlistenverwaltung" wird angezeigt.

Sonderzeichen für Mitgliederlisten

Die folgenden Systemeigenschaften definieren Sonderzeichen, die verwendet werden, um kommagetrennte Werte (CSV) Dateien für Mitgliederlisten zu analysieren.

memberlist.csv.reader.separator

Definiert das Zeichen, das Felder innerhalb einer Zeile der Datei trennt. Das Kommazeichen (,) wird standardmäßig verwendet.

memberlist.csv.reader.quotechar

Definiert das Zeichen, das Feldwerte einschließt, die Leerzeichen oder andere Sonderzeichen enthalten. Die doppelten Anführungszeichen (") werden standardmäßig verwendet.

memberlist.csv.reader.escape

Definiert das in der Datei verwendete Escape-Zeichen. Der Backslash (\) wird standardmäßig verwendet.

Beispiel: Backslash-Zeichen in CSV-Eingabe

Oft enthält die CSV-Eingabe für eine Mitgliederliste Backslashes in Pfadnamen, wie im folgenden Beispiel:

```
Anmeldung, Kategorie, Wert
DOMAIN\Hector_Torres, ResName3, Solaris\HTorres
DOMAIN\Alex_Patrick, Location, Atlanta
```

Standardmäßig betrachtet der CSV-Parser in CA RCM den Backslash als ein Escape-Zeichen. Die sich ergebende Mitgliederliste lässt Backslashes weg:

```
Anmeldung, Kategorie, Wert
DOMAINHector_Torres, ResName3, SolarisHTorres
DOMAINAlex_Patrick, Location, Atlanta
```

Um den Backslash in Feldwerten zuzulassen, bearbeiten Sie die Systemeigenschaft "memberlist.csv.reader.escape", um ein anderes Zeichen als Escape-Zeichen zu definieren.

Hinweis: Wählen Sie ein Escape-Zeichen aus, das nicht in Ihren Daten auftritt. Benutzen Sie die doppelten Anführungszeichen nicht als Escape-Zeichen.

Sofortiges Aufrufen von Genehmigungsvorgängen

Sie können eine Kampagne erstellen, die Genehmigungsaufgaben sofort initiiert, wenn die einzelnen Prüfer Änderungen senden. Die Prüf- und Genehmigungsphasen der Kampagne überschneiden sich. Sowohl die Aktionen zur Zertifizierung als auch zur Änderungsgenehmigung sind großteils während der Kampagne aktiv.

Um Genehmigungsvorgänge sofort aufzurufen, wählen Sie die Option "Sobald jeder Zertifizierer Änderungen sendet" im Fenster "Ausführung" des Assistenten zur Kampagnenerstellung unter "Genehmigungen initiieren".

CA RCM initiiert Prüfungen zu Änderungsgenehmigungen sofort, sobald die Zertifizierer ihre Änderungen senden.

Umgehen von Genehmigungsvorgängen für eine Kampagne

Wenn es nach einer Überprüfung der Zertifizierung zu Änderungen kommt, müssen diese normalerweise von den Eigentümern der betroffenen Entitäten genehmigt werden. Sie können diesen Genehmigungsvorgang in einer Kampagne überspringen. Alle während der Überprüfung der Zertifizierung angezeigten Änderungen werden in CA RCM sofort implementiert.

Wichtig! Durch das Umgehen von Änderungsgenehmigungsüberprüfungen können die Daten in der Zielkonfiguration beschädigt werden. Nur erfahrene Kampagnenmanager sollten nach Absprache mit dem Rollentechniker Kampagnen dieser Art implementieren.

Da Konfigurationsdaten mit hoher Wahrscheinlichkeit versehentlich überschrieben werden, empfehlen wir Ihnen, Genehmigungen nur für Kampagnen zu umgehen, die auf einer Kopie oder einem Teil der Konfigurationsdaten basieren. Verwenden Sie diese Option nicht für Kampagnen, die auf der Modellkonfiguration des aktiven Universums oder einer Originalversion der Konfigurationsdatei basieren.

So umgehen Sie Genehmigungsvorgänge für eine Kampagne:

1. Stellen Sie sicher, dass der Wert der Systemeigenschaft "allowModifiedCampaignProcess" "wahr" ist.

   allowModifiedCampaignProcess

   Gibt an, ob Kampagnenvorgänge, die Genehmigungsaufgaben umgehen, im Portal verfügbar sind.

   Wahr

   Überprüfungsvorgänge, die Genehmigungen umgehen, sind während der Erstellung der Kampagne verfügbar.

   Falsch

   Überprüfungsvorgänge, die Genehmigungen umgehen, werden ausgeblendet. Nur Standardüberprüfungsvorgänge – die Genehmigungen berücksichtigen – können bei der Erstellung einer Kampagne ausgewählt werden.

2. Kopieren Sie eine Konfigurationsdatei oder eine Teildatei, die die entsprechenden Daten enthält.

3. Erstellen Sie eine Kampagne basierend auf der Konfigurationsdatei, die Sie erstellt haben.

4. Deaktivieren Sie im Eigenschafts-Fenster des Assistenten zur Kampagnenerstellung das Kontrollkästchen für die folgende Option:

   Anfrage an Prüfer zu Änderungen

   Initiiert sekundäre Genehmigungsüberprüfung für von Zertifizierern in der Kampagne angeforderte Änderungen.

Auditkartenverletzungen in einer Kampagne

Auditkarten listen Entitäten und Links auf, die "Out-of-Pattern" sind oder Geschäftsprozessregeln verletzen. Diese Informationen können für den Zertifizierer bei der Überprüfung der Entitäten und Links während einer Kampagne nützlich sein.

Wenn Sie eine Kampagne definieren, können Sie Informationen einer Auditkarte im Basisuniversum einschließen oder eine Auditkarte für die Kampagne erstellen. Wenn sich eine Verletzung in der Auditkarte auf eine zu überprüfende Entität bezieht, wird die Entität in den Zertifizierungstickets der Kampagne gekennzeichnet. Zertifizierer können auf das Element klicken, um Details zur Verletzung anzuzeigen.

Anwenden von im Voraus genehmigten Verletzungen in Kampagnen

Wenn eine Liste von im Voraus genehmigten Verletzungen für das Universum angegeben wurde, wird die Liste verwendet, um Verletzungen in allen Kampagnen zu filtern, die sich auf dieses Universum beziehen.

In diesem Fall gibt es zwei Auditkarten: Die Auditkarte, die Sie als Quelle der Verletzungen angeben, wenn Sie die Kampagne erstellen, und die Auditkarte mit im Voraus genehmigten Verletzungen, die Sie für das Universum angeben. Auditkarten-Verletzungen werden folgendermaßen für die Kampagne bearbeitet:

1. CA RCM identifiziert zu überprüfende Entitäten und Links, die in der Auditkarte angezeigt werden, die Sie bei der Erstellung der Kampagne angegeben haben.
2. CA RCM filtert diese Gruppe von Entitäten und Links basierend auf der Auditkarte mit im Voraus genehmigten Verletzungen im Universum. Wenn eine Verletzung aus der Kampagnen-Auditkarte in der im Voraus genehmigten Auditkarte angezeigt wird, wird sie wie für im Voraus genehmigte Verletzungen im Universum konfiguriert: Die Warnung wird entweder ignoriert und nicht angezeigt, oder sie wird ausgegraut.

Weitere Informationen:

Im Voraus genehmigte Verletzungen (siehe Seite 34)

Umfang einer Kampagne

Wenn Sie eine Kampagne erstellen, können Sie Filterkriterien angeben, die die Entitäten und Links der Kampagne einschränken. Die von Ihnen angegebenen Filter können den Charakter der Kampagne beträchtlich ändern und bestimmte Unternehmensanforderungen unterstützen. Zum Beispiel können Sie Kampagnen auf einen Teil der Benutzer oder Ressourcen beschränken, indem Sie Standorte oder andere Attribute verwenden. Sie können auch mehrere Filter mit unterschiedlichen Kriterien kombinieren.

Das Fenster "Filter" (siehe Seite 80) im Assistenten zur Kampagnenerstellung enthält Filteroptionen, die dem Typ der erstellten Kampagne entsprechen.

Filter nach Attributwerten

Sie können Entitäten einer Kampagne mit Entitätsattributwerten filtern.

Sie können auch mehrere attributbasierte Kriterien kombinieren.

Geben Sie diese Filter im Fenster "Filter" des Assistenten zur Kampagnenerstellung an.

Beispiel: Ausstehende Genehmigung für Rollen

Um Rollen zu zertifizieren, die zwar vorgeschlagen, jedoch noch nicht genehmigt worden sind, definieren Sie eine Kampagne zur Rollenzertifizierung mit dem folgenden Entitätsfilter:

- Wählen Sie Rollen mit dem Feld "Genehmigungsstatus" gleich "Genehmigung ausstehend" aus.

Die Kampagne enthält nur Rollen, die noch nicht genehmigt worden sind.

Beispiel: Benutzer-Zertifizierung nach Funktion und Standort

Um die Berechtigungen des Vertriebspersonals in der Region Texas zu zertifizieren, definieren Sie eine Kampagne zur Benutzerzertifizierung mit dem folgenden Entitätsfiltern:

- Wählen Sie Benutzer mit dem Feld "Organisation" gleich "Vertrieb" aus.
- Wählen Sie Benutzer mit dem Feld "Standort" gleich "Texas" aus.
- Aktivieren Sie die Option "Alle Bedingungen".

Die Kampagne berücksichtigt nur Benutzer, die beide Bedingungen erfüllen.

Filter nach Linktypen

Sie können den Umfang einer Kampagne auf gewisse Link-Typen beschränken.

Entitäten in einer Konfiguration können auf drei Arten verknüpft werden:

Direkte Verbindung

Nur ein expliziter, direkter Link verbindet zwei Entitäten. Aufgrund der Vererbung in der Rollenhierarchie von einem übergeordneten auf ein untergeordnetes Element, gibt es zwischen ihnen keine indirekten Links.

Indirekte Verbindung

Zwei Entitäten sind über eine Rolle verknüpft oder über eine Linkvererbung in der Rollenhierarchie von einem übergeordneten auf ein untergeordnetes Element. Es besteht hier kein direkter Link zwischen den Entitäten.

Duale Verbindung

Zwei Entitäten sind sowohl direkt über einen expliziten Link als auch indirekt über die Rollenhierarchie verknüpft.

Geben Sie diese Filter im Fenster "Filter" des Assistenten zur Kampagnenerstellung an. Geben Sie im Bereich "Ausgewählte Links" des Fensters direkte, indirekte und duale Links an, die Sie in die Kampagne aufnehmen wollen. Um Ihre Auswahl zu verfeinern, öffnen Sie die Felder "Direkt", "Indirekt" und "Dual", um eine Baumstruktur der Links zu dem entsprechenden Kampagnentyp, den Sie erstellen, anzuzeigen.

Filter nach Auditkarten

Wenn Sie eine Auditkarte mit der Kampagne verknüpfen, können Sie die Auditkarte zum Filtern der in die Kampagne enthaltenen Links verwenden. Folgende Optionen sind verfügbar:

- Keine Auditkartenfilter – Informationen der Auditkarten werden verwendet, um Verletzungen zu kennzeichnen, jedoch nicht, um den Umfang einer Kampagne zu beschränken.
- Einschließen, wenn in Auditkarte vorhanden – Option zur Erstellung einer Kampagne, die sich auf Verletzungen konzentriert.
- Einschließen, wenn nicht in Auditkarte vorhanden – Prüfer verlieren keine Zeit an Links, die wahrscheinlich gelöscht werden.
- Neue Links vorschlagen – Normalerweise zertifizieren Prüfer die vorhandenen Links zwischen Entitäten in einer Konfiguration. CA RCM kann auch basierend auf der Auditkarte, die mit der Kampagne verknüpft ist, neue Links vorschlagen. Wenn ein Prüfer einen vorgeschlagenen Link genehmigt, wird dieser der Konfiguration hinzugefügt.

Zuvor überprüfte Links

Wenn Sie eine Rezertifizierungs-Kampagne erstellen, können Sie die in die neue Kampagne übernommenen Überprüfungsaufgaben nach dem Status in der alten Kampagne filtern. Wählen Sie im Fenster "Filter" des Assistenten zur Kampagnenerstellung eine der folgenden Optionen unter "Zustände" aus:

Ausstehend

Enthält Linkzertifizierungsaktionen, die nicht in der vorherigen Kampagne beschlossen wurden.

Genehmigt

Enthält Links, die in der vorherigen Kampagne genehmigt wurden.

Abgelehnt

Enthält Links, die in der vorherigen Kampagne abgelehnt wurden.

Hinweis: In Rezertifizierungskampagnen werden keine Kampagnensteuerungsaktionen aus der Referenzkampagne dupliziert. Nur Zertifizierungsaufgaben für Links oder Entitäten werden dupliziert.

Wenn Sie zuvor genehmigte oder abgelehnte Links einschließen, können Sie über die folgenden Optionen steuern, wie die Entscheidungen früherer Prüfer verarbeitet werden.

Auswahl der Genehmiger zurücksetzen

Frühere Überprüfungsentscheidungen werden nicht in die Rezertifizierungskampagne übernommen.

Auswahl der Genehmiger beibehalten

Auswahl des Genehmigers anzeigen

Prüfer der Rezertifizierungskampagne können frühere Überprüfungsentscheidungen anzeigen.

Die folgende Systemeigenschaft steuert, wie überprüfte Links früherer Prüfer in Rezertifizierungskampagnen präsentiert werden.

campaign.settings.recertification.allowOneClickResubmit

Legt fest, ob frühere Überprüfungsentscheidungen als aktive Optionen in Rezertifizierungsaufgaben präsentiert werden. Folgende Werte sind gültig:

Wahr

Vorherige Entscheidungen zur Genehmigung oder Ablehnung werden standardmäßig in Rezertifizierungsaufgaben ausgewählt. Prüfer in der Rezertifizierungskampagne können diese Entscheidungen annehmen, indem Sie im Fenster " Meine Aufgaben" auf "Senden" klicken. Der Assistent zur Kampagnenerstellung zeigt die Option "Auswahl der Genehmiger beibehalten" an.

Falsch

Vorherige Entscheidungen zur Genehmigung oder Ablehnung werden in Rezertifizierungsaufgaben durch grau hinterlegte Symbole angezeigt, diese Entscheidungen sind jedoch nicht standardmäßig ausgewählt. Prüfer in der Rezertifizierungskampagne müssen eine Überprüfungsentscheidung für jeden geprüften Link auswählen. Der Assistent zur Kampagnenerstellung zeigt die Option "Auswahl des Genehmigers anzeigen" an.

Aktualisierte Links

Rezertifizierungs-Kampagnen beziehen sich auf die Überprüfungsaufgaben einer früheren Kampagne. Wenn Sie eine Rezertifizierungs-Kampagne erstellen, können Sie Links in die Konfiguration aufnehmen, die in der früheren Kampagne nicht enthalten waren. Bei diesen Links kann es sich um neue Links handeln, die noch nicht vorhanden waren, als die vorherige Kampagne initiiert wurde, oder um bereits vorhandene Links, die aus der vorherigen Kampagne ausgeschlossen wurden.

Benutzerinformation aus CA Enterprise Log Manager in einer Kampagne

Wenn CA Enterprise Log Manager in Ihrer Umgebung bereitgestellt wird, können in CA RCM von CA Enterprise Log Manager erhaltene Benutzerinformationen in den Tickets einer Kampagne angezeigt werden. Prüfer können diese Informationen verwenden, wenn sie Links zertifizieren.

In Kampagnentickets zeigt ein farbiges Symbol die Häufigkeit der Verwendung an. Prüfer können auf das Symbol klicken, um ein Fenster mit detaillierteren Benutzerinformationen von CA Enterprise Log Manager zu öffnen.

Hinweis: Die Verbindung zwischen CA RCM und CA Enterprise Log Manager wird von einem Sicherheitszertifikat geschützt. Prüfer werden veranlasst, das Sicherheitszertifikat auf ihren Computern zu installieren, wenn sie das erste Mal Informationen aus CA Enterprise Log Manager anzeigen.

Datenabfrage zwischen CA RCM und CA Enterprise Log Manager wird aktiviert und für jedes Universum getrennt konfiguriert. Wenn Sie die Abfrage von CA Enterprise Log Manager für ein Universum aktivieren, zeigen alle auf jenem Universum basierenden Kampagnen Benutzerinformationen an.

Weitere Informationen:

CA Enterprise Log Manager-Integration (siehe Seite 239)

Genehmigungsvorgang auf DNA-Basis

Sie können eine Auditkarte in CA RCM-Client-Tools erstellen, die Änderungen zwischen zwei Konfigurationen widerspiegelt. Wenn Sie die Auditkarte senden, initiiert CA RCM Genehmigungsaktionen für die Änderungen.

Hinweis: Wenn Sie eine Rolle direkt in den Client-Tools löschen, enthält die sich ergebende Auditkarte eine allgemeine Aktion "Rolle löschen" und separate untergeordnete Aktionen für jeden Benutzer, jede Rolle oder jeden Ressourcen-Link, die mit der gelöschten Rolle assoziiert sind. Senden Sie nur die übergeordnete Aktion "Rolle löschen" an den CA RCM-Server. CA RCM generiert automatisch die untergeordneten Aktionen, die mit der Rolle assoziiert sind.

Durchführen eines Upgrades von früheren Versionen

Zertifizierungskampagnen, die Sie mit CA RCM Version 12.5 SP1 oder früher erstellt haben, sind nicht kompatibel mit den Datenschemata, Systemeigenschaften und Steuerelementen zur Kampagneverwaltung dieser Version. Sie können ein Upgrade für diese Kampagnen durchführen und weiterhin mit ihren Daten arbeiten.

- Für 4.x-Versionen und Version 12.0, 12.5 sowie 12.5 SP1 – Verwenden Sie das Fenster "Upgrade der Legacy-Kampagnen" im CA RCM-Portal.
- Für 3.x Versionen – Speichern Sie die Daten in eine Auditkarte und wenden Sie diese Daten auf eine neue Kampagne an.

Hinweis: Weitere Informationen finden Sie in den entsprechenden Abschnitten zu Upgrades im *Installationshandbuch* dieser Version.

Kapitel 7: Verwenden von Dashboards

Dashboards verwenden Grafiken und Diagramme, um einen brauchbaren Überblick über rollenbasierte Konfigurationen und die Ergebnisse statistischer und regelbasierter Analysen zu liefern.

Klicken Sie im Hauptmenü des CA RCM-Portals auf "Dashboards", um auf diese Fenster zuzugreifen.

Einige dieser Fenster werden standardmäßig auf Ihrer Startseite angezeigt.

Je nach Inhalt des Dashboards werden einige oder alle der folgenden Steuerelemente im Dashboard-Kopf angezeigt:

Einstellungen

Öffnet ein Dialogfeld, in dem Sie Datensätze auswählen und in das Dashboard einfügen können.

Anpassen

Öffnet ein Dialogfeld, in dem Sie festlegen können, wie Grafiken und Diagramme angezeigt werden.

Diagramme erstellen

Erstellt die Grafiken und Diagramme des Dashboards neu.

Wert, Prozent

Gibt an, ob in den Grafiken absolute Werte oder Prozente angegeben werden.

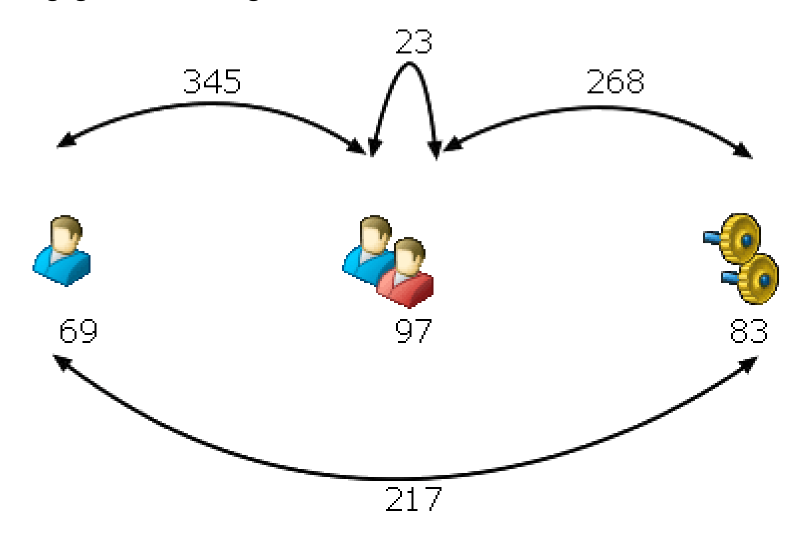
Dieses Kapitel enthält folgende Themen:

Konfigurations-Dashboard

Das Konfigurations-Dashboard ist die Portal-Seite, die eine graphische Übersicht über die Entitäten (Benutzer, Ressourcen und Rollen) einer angegebenen Konfiguration sowie die Verbindungen zwischen diesen bietet.

Die Schaltfläche "Anpassen" ruft das Fenster "Einstellungen" auf, in dem Sie Balken- und Kreisdiagrammparameter festlegen können. Weitere Informationen finden Sie unter Konfigurations-Dashboard-Einstellungen. (siehe Seite 122)

Eine Grafik oben auf der Seite fasst die Benutzer, Ressourcen und Rollen der angegebenen Konfiguration zusammen.



In der angezeigten Konfiguration gibt es 69 Benutzer, 97 Rollen und 83 Ressourcen. Es gibt 345 Benutzer-Rollen-Verbindungen und die Rollenhierarchie enthält 23 Rollen-Rollen-Verbindungen.

Eine Reihe von Balkendiagrammen fasst die Verbindungen zwischen Benutzern, Rollen und Ressourcen zusammen. Die folgenden Linktypen werden beschrieben:

Direkte Verbindung

Nur ein expliziter, direkter Link verbindet zwei Entitäten. Aufgrund der Vererbung in der Rollenhierarchie von einem übergeordneten auf ein untergeordnetes Element, gibt es zwischen ihnen keine indirekten Links.

Indirekte Verbindung

Zwei Entitäten sind über eine Rolle verknüpft oder über eine Linkvererbung in der Rollenhierarchie von einem übergeordneten auf ein untergeordnetes Element. Es besteht hier kein direkter Link zwischen den Entitäten.

Duale Verbindung

Zwei Entitäten sind sowohl direkt über einen expliziten Link als auch indirekt über die Rollenhierarchie verknüpft.

Einstellungen des Konfigurations-Dashboards

Die Balken- und Kreisdiagramme des Konfigurations-Dashboards können vom Benutzer für Anzeigezwecke angepasst werden.

- Balkendiagramme - Die folgenden Parameter können im Balkendiagramm-Histogramm festgelegt werden:
    - Maximale Anzahl - Die maximale Anzahl von angezeigten Histogrammdiagrammbalken.
    - Auto - CA Role & Compliance Manager bestimmt, welche Histrogrammdiagrammmitglieder angezeigt werden.
    - Fix - Legen Sie die gewünschte Anzahl an angezeigten Werten fest im Diagramm fest.
    - Nicht null - Diagrammwerte mit null Mitgliedern nicht anzeigen.
- Kreisdiagramme - Die folgenden Parameter können in den Kreisdiagrammen festgelegt werden:
    - Typ - Wählen Sie 2D- oder 3D-Anzeigetyp aus.
    - Transparenz - Legen Sie den gewünschten angezeigten Transparenzwert mit dem Drop-down-Pfeil fest.
    - Slice-Kontrolle - Bestimmen Sie, wie Kreisdiagramminformationen als Segmente angezeigt werden. Verwenden Sie den Drop-down-Pfeil, um den gewünschten Wert für minimale und maximale Anzahl von Segmenten festzulegen.

Auditkarten-Dashboard

Das Auditkarten-Dashboard ist eine Portalseite, die eine graphische Übersicht über die analytischen Warnungen enthält, die in einer bestimmten Auditkarte aufgezeichnet sind. Der Rollentechniker kann durch die Überprüfung dieser Verletzungen die Güte der Anpassung für die Konfiguration der aktuellen Rolle festlegen und somit entscheiden, wie die Konfiguration verfeinert werden kann.

Hinweis: Das Kriterium der im Auditkarten-Dashboard angezeigten Warnungen spiegelt die Einstellungen der Musteranalyse wider, die zur Erstellung der ausgewählten Auditkarte verwendet wurden. Weitere Informationen zu den Einstellungsoptionen der Musteranalyse finden Sie im "Sage DNA User Guide" (Sage DNA-Benutzerhandbuch).

Compliance-Dashboard

Das Compliance-Dashboard ist eine Portalseite und enthält eine graphische Zusammenfassung möglicher Verletzungen gegen Geschäftsprozessregeln (BPRs).

Normalerweise werden mehrere, mit derselben Konfigurationsdatei verbundene Auditkarten im Dashboard angezeigt. Mit diesen Diagrammen können Sie die Auswirkungen verschiedener BPR-Regelsätze vergleichen und Unternehmensrichtlinien identifizieren, die erhebliche Verletzungen in der Rollenkonfiguration auslösen.

Um Daten im Dashboard anzuzeigen, scrollen Sie zum Ende der Seite, wählen Sie eine Auditkarte aus der CA RCM-Datenbank aus und klicken Sie anschließend auf **Hinzufügen**, um die BPR-Warnungen der Auditkarte in den Diagrammen des Dashboards anzuzeigen.

Hinweis: Das Compliance-Dashboard unterstützt nur Auditkarten, die Warnungen zu Geschäftsprozessregeln (BPRs) enthalten. Nur Warnungen hinsichtlich BPR werden in die Diagramme aufgenommen; auf Muster basierende Warnungen in der Auditkarte werden ignoriert.

Rollenabdeckungs-Dashboard

Das Rollenabdeckungs-Dashboard ist eine Portalseite, die eine grafische Übersicht über die aktuelle Rollenhierarchie bietet und darstellt, inwieweit die Rollenhierarchie den untergeordneten Benutzer-, Ressourcen- und Berechtigungsdaten entspricht.

Die Dashboard-Diagramme zeigen Schwerpunktmaße in zwei Bereichen:

- **Abdeckungsindikatoren** – Welcher Anteil der aktuellen Benutzer- und Ressourcenberechtigungen des Unternehmens sind in der Rollenhierarchie erfasst? Wie vollständig ist die Rollenhierarchie? In welchem Grad werden darin die aktuellen Berechtigungsmuster widergespiegelt?
- **Qualitätsindikatoren** – Wie gut aufgebaut und effizient ist der festgelegte Satz an Rollen und Geschäftsprozessregeln? Welche Rollen verfügen über nur wenige Benutzer oder stehen in Konflikt mit BPRs?

Zertifizierungs-Dashboard

Das Zertifizierungs-Dashboard bietet eine grafische Übersicht über Ihre Zertifizierungskampagnen. Es werden für jede Kampagne Informationen zu genehmigten, abgelehnten, neu zugewiesenen und ausstehenden Überprüfungsaufgaben angezeigt. Informationen zur Leistung von Prüfern und Genehmigern werden aufgelistet.

Sie können Kampagnen nach Typ oder nach Startdatum filtern, und einzelne Kampagnen für das Dashboard auswählen.

Kapitel 8: Self-Service-Aufgaben ausführen

Die Self-Service-Funktion des CA RCM-Portals ermöglicht lokalen Managern sich selbst oder ihre Teammitglieder "on-the-fly" bereitzustellen, indem Links zwischen ihnen bzw. ihren Teammitgliedern und den Rollen und Ressourcen des Unternehmens hinzugefügt oder entfernt werden. Die Self-Service-Aufgabe beinhaltet außerdem die Möglichkeit, neue Rollen zu erstellen oder vorhandene Rollen zu aktualisieren (nur für Manager mit den entsprechenden Berechtigungen). Jede Aufgabe umfasst Funktionen aus mindestens einem Fenster. Details finden Sie in diesem Kapitel.

Unter "Kampagnen hinzufügen" wurde angegeben, dass Manager Entitätenlinks während den Kampagnen nicht aktualisieren. Sie beschränken sich auf die Genehmigung oder Abweisung von aktuellen Links. Manchmal ist es nach einer Kampagne oder nach Änderungen der Bestimmungen und Richtlinien des Unternehmens notwendig, die aktuellen Links zwischen den Benutzern des Unternehmens und den Rollen und Ressourcen des Systems zu aktualisieren bzw. neue Rollen zu erstellen. Dies wird durch die Self-Service-Aufgabe ausgeführt.

Hinweis: Die allgemeinen Funktionen der Fenster zur Aufgabe "Self-Service" wird bereits in Verwenden der CA RCM-Portalbenutzeroberfläche (siehe Seite 17) beschrieben und wird daher in diesem Kapitel nicht erneut aufgenommen.

In diesem Kapitel werden alle über das CA RCM-Portal verfügbaren Self-Service-Aufgaben beschrieben. Manager haben nur auf die Funktionen Zugriff, für die sie bereitgestellt wurden. In diesem Handbuch werden die Self-Service-Aufgaben in zwei Gruppen aufgeteilt:

Bereitstellungsaufgaben

Umfasst alle Aufgaben, die Benutzerrollen oder -ressourcen verwalten:

- Rollenzuweisungen meines Teams verwalten
- Meine Rollenzuweisungen verwalten
- Ressourcenzuweisungen meines Teams verwalten
- Meine Ressourcenzuweisungen verwalten

Rollendefinierende Aufgaben

Umfasst die folgenden Aufgaben zur Rollendefinition:

- Neue Rollendefinition anfragen
- Änderungen einer Rollendefinition anfragen

Hinweis: Wenn Sie eine Self-Service-Aufgabe durchführen möchten, die nicht im Self-Service-Menü angezeigt wird, wenden Sie sich an Ihren Systemadministrator.

Das CA RCM-Portal ermöglicht Ihnen, Links zu ihren beliebtesten Self-Service-Aufgaben auf der Startseite unter "Meine Geschäftsprozesse" hinzuzufügen.

Dieses Kapitel enthält folgende Themen:

Allgemeine Funktionen – Self-Service

Die Funktionen für Self-Service hängen von der ausgeführten Aufgabe ab. Es gibt jedoch einige Funktionen, die bei mehreren Aufgaben vorhanden sind.

In diesem Abschnitt werden zwei dieser Funktionen beschrieben:

- Testen der Compliance
- Entitäten vorschlagen

Hier muss erwähnt werden, das obwohl Sie eine Liste mit empfohlenen Entitäten mittels "Entitäten vorschlagen" erhalten, der Dienst "Compliance testen" dennoch feststellt, dass die vorgeschlagenen Links gegen die BPRs des Systems verstoßen. Dies erklärt sich aus der Tatsache, dass der Dienst "Entitäten vorschlagen" einer analytischen, auf Mustern basierenden Technologie zugrundeliegt, die Funktion "Compliance testen" jedoch die von Systemadministratoren geschriebenen Regeln überprüft. Diese Regeln übergehen möglicherweise die Ergebnisse der analytischen, auf Mustern basierenden Überprüfung der Konfigurationsdateien des Unternehmens.

So wird zum Beispiel einer Gruppe von Benutzern eine bestimmte Anwendungsrolle unter bestimmten Bedingungen empfohlen, die Funktion "Compliance testen" erkennt dies jedoch als Verletzung an, da die Anwendung eine Lizenz erfordert und zu diesem Zeitpunkt keine freien Lizenzen vorhanden sind.

Weitere Informationen:

Testen der Compliance (siehe Seite 127)
Wie CA RCM Entitäten vorschlägt (siehe Seite 128)

Testen der Compliance

Bei einer Self-Service-Bereitstellungsaufgabe können Sie die Übereinstimmung Ihrer Auswahl mit bestehenden BPRs, Sicherheitsbestimmungen und Richtlinien überprüfen.

Hinweis: Weitere Informationen zu Verletzungen, die auf Non-Compliance und andere Sicherheitsprobleme zurückzuführen sind, finden Sie im *DNA User Manual (DNA-Benutzerhandbuch)*.

Das Fenster "Verletzungen" listet Linkentitäten auf, die eine Verletzung aufweisen. Wenn keine Verletzungen vorhanden sind, werden keine Datensätze aufgelistet.

Im Fenster "Verletzungen" werden Entitäten nach Regel oder Musterbedingung, die die Verletzung ausgelöst haben, gruppiert. Alle Linkentitäten, die eine bestimmte Regel oder ein bestimmtes Muster verletzen, werden zusammen aufgelistet. Zusätzlich zu Linkinformationen wird das folgende Feld für jede Entität angezeigt:

Bewertung

Das für eine bestimmte BPR definiertes Risiko. Der Wert liegt üblicherweise zwischen 0 und 100.

So führen Sie einen Compliance-Test aus

1. Klicken Sie auf "Compliance testen". Das Fenster "Verletzungen" wird in einem separaten Browserfenster geöffnet.
2. Klicken Sie in der oberen rechten Ecke auf ✖, um das Fenster zu schließen.

Wie CA RCM Entitäten vorschlägt

Sie können CA RCM-Mustererkennungsalgorithmen verwenden, um neue Berechtigungen für sich selbst, für Ihr Team oder für Rollen vorzuschlagen, die Sie verwalten.

Wenn Sie zum Beispiel die Rollenzuweisungen Ihres Teams überprüfen, können Sie auf "Rollen vorschlagen" klicken, um anhand der Musteranalyse eine gewichtete Liste von Rollen zu generieren.

Hinweis: Weitere Informationen über CA RCM-Mustererkennung finden Sie im *DNS-Benutzerhandbuch*.

Die Vorschläge von CA RCM basieren auf mehreren Algorithmen. Je nachdem, welche Self-Service-Anfrage aktiv ist, sind die folgenden Algorithmen verfügbar:

Übereinstimmende Rechte

CA RCM findet Rollen mit Rechten, die (zu einem bestimmten Prozentsatz) mit denen einer Referenzrolle übereinstimmen. Dieser Algorithmus ist gleichwertig mit der Option "In/Out of Pattern: User matching" im DNA-Client-Tool.

HR-Muster

CA RCM findet Berechtigungen, die Benutzern mit ähnlichen HR-Attributwerten zugewiesen sind. Dieser Algorithmus ist gleichwertig mit der Option "In/Out of Pattern: Propose new roles for users (by Human Resources)" im DNA-Client-Tool.

Berechtigungsmuster

Vergleicht die Berechtigungen der aktuellen Benutzer mit einem allgemeinen Muster von Berechtigungen in der Konfiguration. Dieser Algorithmus ist gleichwertig mit der Option "In/Out of Pattern: Propose new roles for users (by Privileges)" im DNA-Client-Tool.

Übereinstimmende Regel

Findet Benutzer, auf die die Regel zutrifft, die verwendet wird, um eine Rolle denjenigen zuzuweisen, die die Rolle noch nicht haben. Dieser Algorithmus ist gleichwertig mit der Option "In/Out of Pattern: Identify users matching rule based roles" im DNA-Client-Tool.

Diese Algorithmen schlagen Entitäten vor, die sowohl auf direkten als auch auf indirekten Links basieren.

Die mit Mustern übereinstimmenden Ergebnisse werden in der Spalte der entsprechenden Tabelle angezeigt:

- Für Bereitstellungsaufgaben werden die Ergebnisse in der Tabelle "Andere Rollen" angezeigt.
- Für Aufgaben zur Rollendefinition werden die Ergebnisse in einer der entsprechenden Entität zugewiesenen Tabelle angezeigt.

Wenn Sie Vorschläge für mehr als einen Benutzer anfordern, wird in der Tabelle angegeben, wie viele Benutzer der ausgewählten Benutzern übereinstimmen ([übereinstimmend]/[ausgewählt]).

Klicken Sie auf "[Entität] vorschlagen", um diesen Dienst als Teil einer Bereitstellungsaufgabe zu aktivieren. Die Tabelle, in der die Schaltfläche zu finden ist, ändert sich je nach Entität und enthält die folgenden Spalten:

Dienst	Hinzugefügte Spalten
Rollen vorschlagen	Vier Spalten für Muster und zwei Spalten mit Details.
Ressourcen vorschlagen	■ Für Fenster zur Bereitstellungsaufgabe: Zwei Spalten für Muster und eine Spalte mit Details. ■ Für Fenster zur Rollendefinitionsaufgabe: die Spalte "Eingeschrieben"
Benutzer vorschlagen	Die Spalte "Eingeschrieben".

Klicken Sie in einem Fenster der Bereitstellungsaufgabe auf einen hervorgehobenen Link in der Spalte "Details", um weitere Informationen zu den Benutzern und den Übereinstimmungen mit bestimmten Rollen/Ressourcen in einem separaten Browserfenster anzuzeigen.

Klicken Sie in der oberen rechten Ecke auf, um das Fenster zu schließen.

Die Spalte "Eingeschrieben", die in dem Fenster der Rollendefinitionsaufgabe angezeigt wird, enthält die Anzahl der ausgewählten Benutzer/Ressourcen, die mit dieser Ressource oder diesem Benutzer verlinkt ist.

Rollenzuweisungen meines Teams verwalten

Im Rahmen des <rohem>-Portals besteht Ihr Team hauptsächlich aus den Benutzern, denen Sie als Manager zugewiesen sind. Als Team-Manager müssen Sie möglicherweise aufgrund von Unternehmensänderungen, Änderungen des Mitarbeiterstamms oder infolge eines Auditprozesses die Rollenzuweisungen aktualisieren. Das Fenster "Rollen meines Teams verwalten" (MMT-Rolle) ermöglicht Ihnen, die Rollen Ihres Teams zu verwalten. Sie können die Einschreibung Ihres Teams in eine oder mehrere Rollen anfragen oder Links zwischen ausgewählten Benutzern und deren aktuellen Rollen trennen.

Das Hilfsprogramm "Rollenmanagement" ermöglicht es Ihnen, manuell eine spezifische Zielrolle auszuwählen, bietet Ihnen darüber hinaus eine Liste vorgeschlagener Rollen sowie deren auf Mustern basierendes Verhalten und stellt Ihnen so die nötigen Informationen zur Verfügung, um eine informierte Auswahl zu treffen.

Das Fenster ist in vier Abschnitte unterteilt:

Allgemein

Bietet beschreibende Informationen zur laufenden Aktion.

Benutzer

Ihre Teammitglieder Wählen Sie einen oder mehrere Benutzer für die aktuelle Aktion aus.

Aktuell eingeschriebene Rollen

Mit den ausgewählten Benutzern verknüpfte aktuelle Rollen.

Andere Rollen

Empfohlene Rollen für die ausgewählten Benutzer.

Die Abschnitte "Benutzer" und "Andere Rollen" bieten anpassbare Tabellen.

Da das Fenster "MMT-Rolle" viele Optionen und große Flexibilität bietet, wird der Prozess der Aufgabe nach Abschnitten aufgegliedert:

- Die Felder im Abschnitt "Allgemein"
- Die Optionen und Funktionen der Tabelle "Benutzer"
- Die Optionen und Funktionen der Tabelle "Aktuell eingeschriebene Rollen"
- Die Optionen und Funktionen der Tabelle "Andere Rollen"

Um die Rollenzuweisungen Ihres Teams zu verwalten, klicken Sie im Self-Service-Menü auf "Rollenzuweisungen meines Teams verwalten". Das Fenster "Rollen meines Teams verwalten" wird geöffnet.

Weitere Informationen:

Abschnitt "Allgemein" (Fenster MMT-Rolle) (siehe Seite 132)
Tabelle "Benutzer" (Fenster MMT-Rolle) (siehe Seite 133)
Tabelle "Aktuell eingeschriebene Rollen" (Fenster "Meine Rollen verwalten") (siehe Seite 135)
Tabelle "Andere Rollen" (Fenster MMT-Rolle) (siehe Seite 136)

Abschnitt "Allgemein" (Fenster MMT-Rolle)

Der Abschnitt "Allgemein" des Fensters "Rollen meines Teams verwalten" enthält die folgenden Felder:

Universum

Wählen Sie das Universum aus, mit dem Sie arbeiten möchten. Die Tabelle und die verfügbaren Rollen des Benutzers hängen vom Universum ab.

Geschäftsbereich

Allgemeine Informationen (beschreibend). Diese Information wird im Feld "Beschreibung" des folgenden Self-Service-Genehmigungsstammtickets angezeigt.

Geschäftsprozess

Allgemeine Informationen (beschreibend). Diese Information wird im Feld "Beschreibung" des folgenden Self-Service-Genehmigungsstammtickets angezeigt.

Beschreibung

Geben Sie eine genaue und sinnvolle Beschreibung der Änderungen ein, die sie an den Rollen Ihres Teams vornehmen möchten.

Senden

Klicken Sie auf "Senden", um Änderungen anzufragen.

So geben Sie Daten im Abschnitt "Allgemein" (MMT-Rolle) ein

1. Wählen Sie ein Universum in der Dropdown-Liste aus.
2. Geben Sie den Geschäftsbereich für die aktuelle Aktion ein.
3. Geben Sie den Geschäftsprozess ein, der mit der aktuellen Aktion verbunden ist.
4. Geben Sie eine Beschreibung ein.

Tabelle "Benutzer" (Fenster MMT-Rolle)

Die Tabelle "Benutzer" zeigt eine Liste der Benutzer in den Konfigurationsdateien des ausgewählten Universums an. Die Mitglieder Ihres Teams sind mir einem grünen Punkt neben ihrer Personen-ID markiert.

Die Tabelle "Benutzer" bietet die folgenden Optionen:

Hinzufügen

Eine Spalte mit Kontrollkästchen, eines pro Benutzer. Wählen Sie eines oder mehrere aus. Wenn Sie mehrere Benutzer auswählen, werden alle Änderungen, die Sie vornehmen, für alle ausgewählten Benutzer implementiert.

Personen-ID

Klicken Sie auf eine hervorgehobene ID, der in dieser Spalte erscheint, um die entsprechende Benutzerkarte zu öffnen.

Rollen abrufen

Bietet eine Liste der aktuell eingeschriebenen Rollen für die ausgewählten Benutzer.

Anpassen

Ermöglicht es Ihnen, die Spalten festzulegen, die in der Tabelle "Benutzer" angezeigt werden.

Datensätze pro Seite

Wählen Sie die Anzahl an Datensätzen, die in der Tabelle "Benutzer" angezeigt werden.

Benutzer suchen

Öffnet das Filterfenster "Benutzer auswählen", um Sie bei der Suche nach spezifischen Benutzern zu unterstützen.

Wenn Sie die Benutzer ausgewählt haben, die sie jetzt verwalten möchten, könne sie auf "Rollen abrufen" klicken, um eine Liste der aktuell mit diesen Benutzern verbundenen Rollen zu erhalten.

Hinweis: Wenn die Aktionen, die Sie unternehmen wollen, die aktuell mit dem ausgewählten Benutzer verlinkten eingeschrieben Rollen nicht einbeziehen, können Sie die Tabelle "Aktuell eingeschriebene Rollen" überspringen und zur Tabelle "Andere Rollen" wechseln.

So wählen Sie Benutzer aus und erhalten ihre Rollen

1. Wählen Sie einen oder mehrere Benutzer in der Tabelle "Benutzer" aus. Sie können auf "Benutzer suchen" klicken, um das Fenster "Benutzer auswählen" zu öffnen.
2. Auf "Rollen abrufen" klicken.

   Die mit den ausgewählten Benutzern verknüpften Rollen werden in der Tabelle "Aktuell eingeschriebene Rollen" angezeigt. Eine Liste der Rollen, die nicht mit den aktuell ausgewählten Benutzern verknüpft sind, werden in der Tabelle "Andere Rollen" angezeigt.

   Jetzt können Sie aus folgenden Möglichkeiten auswählen:

   - Die aktuelle Einschreibungsliste verwalten
   - Zusätzliche Rollen für die ausgewählten Benutzer hinzufügen
   - Beide ausführen.

   Wenn sie die aktuell eingeschrieben Rollen nicht verwalten möchten, fügen Sie den ausgewählten Benutzern Rollen hinzu.

Tabelle "Aktuell eingeschriebene Rollen" (Fenster "Meine Rollen verwalten")

Dieser Abschnitt ermöglicht es Ihnen, die aktuelle Einschreibung von Rollen für Ihre ausgewählten Benutzer zu verwalten. Die Optionen, die Ihnen zur Verfügung stehen, hängen davon ab, wie viele Benutzer Sie für die aktuelle Aktion ausgewählt haben.

Wenn nur ein Benutzer ausgewählt ist, klicken Sie auf "Rollen abrufen", um eine Liste der mit diesem ausgewählten Benutzer verknüpften Rollen zu erhalten.

In diesem Fall steht Ihnen nur eine mögliche Option zur Verfügung: Das Kontrollkästchen "Entfernen" neben der Rolle aktivieren und damit den Link zwischen Benutzer und der ausgewählten Rolle trennen.

Wenn Sie mehr als einen Benutzer auswählen, bietet Ihnen die Tabelle "Aktuell eingeschriebene Rollen" eine zusätzliche Spalte: Einschreibung.

Wenn mehrere Benutzer ausgewählt sind, können Sie:

- Das Kontrollkästchen "Entfernen" neben der Rolle aktivieren und damit damit den Link zwischen Benutzer und der ausgewählten Rolle trennen.
- Das Kontrollkästchen "Hinzufügen" neben einer Rolle aktivieren, bei der nur einige der ausgewählten Benutzer eingeschrieben sind und damit alle ausgewählten Benutzer mit der ausgewählten Rolle verknüpfen.

Die Tabelle "Aktuell eingeschriebene Rollen" bietet folgende Optionen:

Hinzufügen

Eine Spalte mit Kontrollkästchen, eines pro Rolle. Wählen Sie eines oder mehrere aus. Kontrollkästchen neben Rollen, die bereits mit allen ausgewählten Benutzern verknüpft sind, sind nicht aktiv.

Entfernen

Eine Spalte mit Kontrollkästchen, eines pro Rolle. Aktivieren Sie eines oder mehrere, um den Link zwischen dem ausgewählten Benutzer und den ausgewählten Rollen zu entfernen.

Einschreibung

Diese Spalte wird nur dann angezeigt, wenn mehrere Benutzer ausgewählt sind. Zeigt numerisch an [Anzahl der eingeschriebenen Benutzer]/[Gesamtanzahl der ausgewählten Benutzer], 2/3 bedeutet zum Beispiel, dass zwei der drei ausgewählten Benutzer bei dieser Rolle eingeschrieben sind. Diese Spalte gibt den Wert auch als Prozentsatz an, z. B. 1/3 (33%).

Rollenname

Klicken Sie auf einen hervorgehobenen Rollennamen, der in dieser Spalte erscheint, um seine Rollenkarte zu öffnen.

Je nachdem, welche Aktion Sie ausführen möchten, haben Sie die Aufgabe möglicherweise nach dem Aktivieren der entsprechenden Kontrollkästchen bereits abgeschlossen. In diesem Fall können Sie den Abschnitt "Andere Rollen" ignorieren und Ihre Anfragen mit einem Klick auf "Senden" unten im Fenster "Rollen meines Teams verwalten" senden.

Um in der Tabelle "Aktuell eingeschriebene Rollen" eine Auswahl zu treffen, klicken Sie in dieser Tabelle auf die entsprechenden Kontrollkästchen in der Spalte "Hinzufügen" bzw. "Entfernen".

Jetzt können Sie aus folgenden Möglichkeiten auswählen:

- Den Prozess hier abbrechen
- Zusätzliche Rollen für die ausgewählten Benutzer hinzufügen

Wenn Sie keine neuen Rollen hinzufügen möchten, senden Sie Ihre Anfragen.

Tabelle "Andere Rollen" (Fenster MMT-Rolle)

Dieser Abschnitt ermöglicht es Ihnen, Ihre ausgewählten Benutzer bei zusätzlichen Rollen Ihrer Wahl einzuschreiben. Die Einschreibung an sich erfolgt nach einem Überprüfungsprozess.

Hinweis: Wenn Sie im Abschnitt "Benutzer" auf "Rollen abrufen" klicken, wird in der Tabelle "Andere Rollen" eine Liste der Rollen angezeigt, die nicht mit den aktuell ausgewählten Benutzern verknüpft sind.

Über die Verwaltung der aktuell mit Mitgliedern Ihres Teams verknüpften Rollen hinaus können Sie eine Liste der für Ihre ausgewählten Benutzer empfohlenen Rollen vom System anfordern. Die Liste der Rollen wird im Abschnitt "Andere Rollen" angezeigt.

Der Abschnitt "Andere Rollen" bietet Ihnen die folgenden Optionen:

Hinzufügen

Eine Spalte mit Kontrollkästchen, eines pro Rolle. Wählen Sie eines oder mehrere aus, um die ausgewählten Benutzer mit zusätzlichen Rollen zu verknüpfen.

Rollenname

Klicken Sie auf einen hervorgehobenen Rollennamen, der in dieser Spalte erscheint, um seine Rollenkarte zu öffnen.

Anpassen

Ermöglicht es Ihnen, die Spalten festzulegen, die in der Tabelle "Andere Rollen" angezeigt werden.

Datensätze pro Seite

Wählen Sie die Anzahl an Datensätzen, die in der Tabelle "Andere Rollen" pro Seite angezeigt werden.

Rollen suchen

Öffnet das Filterfenster "Rolle auswählen", um Sie bei der Suche nach spezifischen Rollen zu unterstützen.

Testen der Compliance

Überprüft, ob die in der Tabelle "Andere Rollen" vorgenommene Auswahl den bestehenden Richtlinien und BPRs (Geschäftsprozessregeln) entspricht.

Rollen vorschlagen

Bietet eine Liste möglicher Rollen auf der Basis der CA RCM-Mustererkennungs-Technologie.

Diese Tabelle bietet Ihnen mehrere Optionen:

- Sie können manuell eine oder mehrere Rollen auswählen, die Sie mit den ausgewählten Benutzern verknüpfen möchten.
- Sie können die Option "Rollen suchen" verwenden, um spezifische Rollen zu suchen, und dann eine Auswahl in der gefilterten Rollenliste treffen.
- Sie können auf "Rollen vorschlagen" klicken und die in dieser Funktion angebotenen Informationen nutzen, um Rollen mit den ausgewählten Benutzern zu verknüpfen.

Nachdem Sie Ihre Auswahl getroffen haben, können Sie die Übereinstimmung Ihrer Auswahl mit bestehenden BPRs und Richtlinien überprüfen.

Sie können entscheiden, ob Sie die Anfrage trotz der aufgeführten Nichtübereinstimmungen ausführen, oder ob Sie Ihre Auswahl ändern.

Wichtig! Bitte bedenken Sie bei der Auswahl mehrerer Benutzer, dass jede rollenbezogene Auswahl auf alle Benutzer gleich angewendet wird. Wenn Sie die Auswahl der Benutzer ändern, klicken Sie erneut auf "Rollen abrufen".

So verknüpfen Sie Rollen mit ausgewählten Benutzern

1. Scrollen Sie im Fenster "Rollen meines Teams verwalten" nach unten zur Tabelle "Andere Rollen".
2. (Optional) Klicken Sie auf "Rollen suchen", um zum Filterfenster "Rolle auswählen" zu gelangen.
3. (Optional) Klicken Sie auf "Rollen vorschlagen", um die Vorschläge des CA RCM-Portals anzuzeigen.
4. Wählen Sie eine oder mehrere Rollen aus, um sie mit den ausgewählten Benutzern zu verknüpfen.
5. (Optional) Klicken Sie auf "Compliance testen", um Ihre Auswahl auf mögliche Verletzungen hin zu überprüfen.

   Das Fenster "Verletzungen" wird in einem separaten Browserfenster geöffnet.
6. Klicken Sie auf X, um das Fenster "Verletzungen" zu schließen.
7. Klicken Sie auf "Senden".

   Das Fenster "Anfrage" wird angezeigt.

Weitere Informationen:

Testen der Compliance (siehe Seite 127)
Wie CA RCM Entitäten vorschlägt (siehe Seite 128)
Einführung in die Anfragentabellen (siehe Seite 169)

Meine Rollenzuweisungen verwalten

Als Benutzer müssen Sie möglicherweise aufgrund von Unternehmensänderungen, Änderungen des Mitarbeiterstamms oder infolge eines Auditprozesses eine Aktualisierung Ihrer Rollen anfordern. Das Fenster "Meine Rollenzuweisungen verwalten" ermöglicht es Ihnen, Ihre Rollen zu verwalten, indem Sie eine Anfrage für das Hinzufügen neuer Rollen erstellen oder bestehende Rollen löschen.

Das Hilfsprogramm "Rollenmanagement" ermöglicht Ihnen, eine bestimmte Zielrolle auszuwählen. Sie erhalten auch Rollen als Vorschlag und die notwendigen Informationen, um eine informierte Auswahl zu treffen.

Das Fenster ist in drei Abschnitte unterteilt:

Allgemein

Bietet beschreibende Informationen zur laufenden Aktion.

Aktuell eingeschriebene Rollen

Mit den ausgewählten Benutzern verknüpfte aktuelle Rollen.

Andere Rollen

Eine Liste verfügbarer Rollen.

Der Abschnitt "Andere Rollen" zeigt eine anpassbare Tabelle an:

Da das Fenster "Meine Rollen verwalten" viele Optionen und große Flexibilität bietet, werden die Prozeduren nach Abschnitten aufgegliedert:

- Die Felder im Abschnitt "Allgemein"
- Die Optionen und Funktionen der Tabelle "Aktuell eingeschriebene Rollen"
- Die Optionen und Funktionen der Tabelle "Andere Rollen"

Um Ihre Rollenzuweisungen zu verwalten, klicken Sie im Self-Service-Menü auf "Meine Rollenzuweisungen verwalten". Das Fenster "Meine Rollen verwalten" wird geöffnet.

Weitere Informationen:

Abschnitt "Allgemein" (Fenster "Meine Rollen verwalten") (siehe Seite 140)
Tabelle "Aktuell eingeschriebene Rollen" (Fenster "Meine Rollen verwalten") (siehe Seite 141)
Tabelle "Andere Rollen" (Fenster "Meine Rollen verwalten") (siehe Seite 143)

Abschnitt "Allgemein" (Fenster "Meine Rollen verwalten")

Der Abschnitt "Allgemein" des Fensters "Meine Rollen verwalten" enthält die folgenden Felder:

Universum

Wählen Sie das Universum aus, mit dem Sie arbeiten möchten. Die Tabelle und die verfügbaren Rollen des Benutzers hängen vom Universum ab.

Geschäftsbereich

Allgemeine Informationen (beschreibend). Diese Information wird im Feld "Beschreibung" des folgenden Self-Service-Genehmigungsstammtickets angezeigt.

Geschäftsprozess

Allgemeine Informationen (beschreibend). Diese Information wird im Feld "Beschreibung" des folgenden Self-Service-Genehmigungsstammtickets angezeigt.

Beschreibung

Geben Sie eine genaue und sinnvolle Beschreibung der Änderungen ein, die sie an Ihren Rollen vornehmen möchten.

Senden

Klicken Sie auf "Senden", um Änderungen anzufragen.

So geben Sie Daten im Abschnitt "Allgemein" von "Meine Rollen verwalten" ein

1. Wählen Sie ein Universum in der Dropdown-Liste aus.

   Die Tabelle "Aktuell eingeschriebene Rollen" und die Tabelle "Andere Rollen" zeigen Ressourcen an, die der Konfiguration des ausgewählten Universums angehören.

2. Geben Sie den Geschäftsbereich für die aktuelle Aktion ein.
3. Geben Sie den Geschäftsprozess ein, der mit der aktuellen Aktion verbunden ist.
4. Geben Sie eine Beschreibung ein.

Hinweis: Wenn die Aktionen, die Sie unternehmen wollen, nicht Ihre aktuell eingeschrieben Rollen mit einbeziehen, können Sie die Tabelle "Aktuell eingeschriebene Rollen" überspringen und zur Tabelle "Andere Rollen" wechseln.

Wenn sie die aktuell eingeschrieben Rollen nicht verwalten möchten, fügen Sie den ausgewählten Benutzern Rollen hinzu.

Weitere Informationen:

Tabelle "Aktuell eingeschriebene Rollen" (Fenster "Meine Rollen verwalten") (siehe Seite 141)
Tabelle "Andere Rollen" (Fenster "Meine Rollen verwalten") (siehe Seite 143)

Tabelle "Aktuell eingeschriebene Rollen" (Fenster "Meine Rollen verwalten")

Dieser Abschnitt ermöglicht es Ihnen, Ihre aktuell eingeschriebenen Rollen zu verwalten. Als Sie das Universum ausgewählt haben, hat Ihnen das Portal CA RCM eine Liste Ihrer aktuellen Rollen innerhalb der Konfiguration des Universums zur Verfügung gestellt.

Die Tabelle "Aktuell eingeschriebene Rollen" bietet nur eine Option für die Aufgabe "Meine Rollen verwalten": ein Kontrollkästchen "Entfernen" neben der Rolle zu aktivieren und damit den Link zwischen Ihnen und der ausgewählten Rolle zu trennen.

Die Tabelle "Aktuell eingeschriebene Rollen" bietet folgende Funktionen:

Hinzufügen

Eine Spalte mit Kontrollkästchen, eines pro Rolle. Diese Spalte ist in diesem Fenster inaktiv.

Entfernen

Eine Spalte mit Kontrollkästchen, eines pro Benutzer. Aktivieren Sie eines oder mehrere, um den Link zwischen dem ausgewählten Benutzer und den ausgewählten Rollen zu entfernen.

Rollenname

Klicken Sie auf einen hervorgehobenen Rollennamen, der in dieser Spalte erscheint, um seine Rollenkarte zu öffnen.

Je nachdem, welche Aktion Sie ausführen möchten, haben Sie die Aufgabe möglicherweise nach dem Aktivieren der entsprechenden Kontrollkästchen bereits abgeschlossen. In diesem Fall können Sie die Anweisungen in "Andere Rollen" ignorieren und Ihre Anfragen mir einem Klick auf "Senden" unten im Fenster "Meine Rollen verwalten" senden.

Um in der Tabelle "Aktuell eingeschriebene Rollen" eine Auswahl zu treffen, aktivieren Sie die entsprechenden Kontrollkästchen in der Spalte "Entfernen" der Tabelle "Aktuell eingeschriebene Rollen".

Jetzt können Sie aus folgenden Möglichkeiten auswählen:

- Den Prozess hier abbrechen
- Rollen hinzufügen.

Wenn Sie keine neuen Rollen hinzufügen möchten, senden Sie Ihre Anfragen.

Weitere Informationen:

Tabelle "Andere Rollen" (Fenster "Meine Rollen verwalten") (siehe Seite 143)

Tabelle "Andere Rollen" (Fenster "Meine Rollen verwalten")

Dieser Abschnitt ermöglicht es Ihnen, sich bei zusätzlichen Rollen Ihrer Wahl einzuschreiben. Die Einschreibung an sich erfolgt nach einem Überprüfungsprozess.

Über die Verwaltung der Rollen, mit denen Sie derzeit verbunden sind, hinaus können Sie eine Liste der für Sie selbst empfohlenen Rollen vom System anfordern. Die Liste der Rollen wird im Abschnitt "Andere Rollen" angezeigt.

Der Abschnitt "Andere Rollen" bietet Ihnen die folgenden Optionen:

Hinzufügen

Eine Spalte mit Kontrollkästchen, eines pro Rolle. Wählen Sie eines oder mehrere aus.

Rollenname

Klicken Sie auf einen hervorgehobenen Rollennamen, der in dieser Spalte erscheint, um seine Rollenkarte zu öffnen.

Anpassen

Ermöglicht es Ihnen, die Spalten festzulegen, die in der Tabelle "Andere Rollen" angezeigt werden.

Datensätze pro Seite

Wählen Sie die Anzahl an Datensätzen, die in der Tabelle "Andere Rollen" pro Seite angezeigt werden.

Rollen suchen

Öffnet das Filterfenster "Rolle auswählen", um Sie bei der Suche nach spezifischen Rollen zu unterstützen.

Testen der Compliance

Überprüft, ob die in der Tabelle "Andere Rollen" vorgenommene Auswahl bestehenden Richtlinien und BPRs (Geschäftsprozessregel) entspricht.

Rollen vorschlagen

Bietet eine Liste möglicher Rollen auf der Basis der CA RCM-Mustererkennungs-Technologie.

Diese Tabelle bietet Ihnen mehrere Optionen:

- Sie können manuell eine oder mehrere Rollen auswählen, bei denen Sie sich einschreiben möchten.
- Sie können die Option "Rollen suchen" verwenden, um spezifische Rollen zu suchen, und dann eine Auswahl in der gefilterten Rollenliste treffen.
- Sie können auf "Rollen vorschlagen" klicken und die in dieser Funktion angebotenen Informationen nutzen, um Rollen zu finden, bei denen Sie sich einschreiben sollten.

Nachdem Sie Ihre Auswahl getroffen haben, können Sie die Übereinstimmung Ihrer Auswahl mit bestehenden BPRs und Richtlinien überprüfen.

Sie können entscheiden, ob Sie die Anfrage trotz Nichtübereinstimmung ausführen, oder ob Sie Ihre Auswahl ändern.

So verknüpfen Sie mit zusätzlichen Rollen

1. Im Fenster "Meine Rollen verwalten" scrollen Sie nach unter zur Tabelle "Andere Rollen".
2. (Optional) Klicken Sie auf "Rollen suchen", um zum Filterfenster "Rolle auswählen" zu gelangen.
3. (Optional) Klicken Sie auf "Rollen vorschlagen", um die Vorschläge des CA RCM-Portals anzuzeigen.
4. Wählen Sie eine oder mehrere Rollen aus, um sie mit den ausgewählten Benutzern zu verknüpfen.
5. (Optional) Klicken Sie auf "Compliance testen", um Ihre Auswahl auf mögliche Verletzungen hin zu überprüfen.

   Das Fenster "Verletzungen" wird in einem separaten Browserfenster geöffnet. Klicken Sie auf X, um das Fenster "Verletzungen" zu schließen.
6. Klicken Sie auf "Senden".

   Das Fenster "Anfrage" wird angezeigt.

Weitere Informationen:

Testen der Compliance (siehe Seite 127)
Wie CA RCM Entitäten vorschlägt (siehe Seite 128)
Einführung in die Anfragentabellen (siehe Seite 169)

Die Ressourcen meines Teams verwalten

Im Rahmen des <rohem>-Portals besteht Ihr Team hauptsächlich aus den Benutzern, denen Sie als Manager zugewiesen sind. Als Team-Manager müssen Sie möglicherweise aufgrund von Unternehmensänderungen, Aktualisierung von Ressourcen oder infolge eines Auditprozesses die Ressourcen aktualisieren. "Die Ressourcen meines Teams verwalten" (MMT-Ressourcen) ermöglicht es Ihnen, die Ressourcen Ihres Teams zu verwalten:

- Indem Sie eine Anfrage für das Hinzufügen neuer Ressourcen erstellen, entweder für einen spezifischen Benutzer oder für eine Benutzergruppe
- Indem Sie den Link zwischen ausgewählten Benutzern und deren aktuellen Ressourcen trennen

Das Hilfsprogramm "Ressourcen-Management" ermöglicht es Ihnen, manuell eine spezifische Zielressource auszuwählen, bietet Ihnen darüber hinaus eine Liste vorgeschlagener Ressourcen und deren auf Mustern basierendes Verhalten und stellt Ihnen so die nötigen Informationen zur Verfügung, um eine informierte Auswahl zu treffen.

Das Fenster ist in vier Abschnitte unterteilt:

Allgemein

Bietet beschreibende Informationen zur laufenden Aktion.

Benutzer

Ihre Teammitglieder Wählen Sie einen oder mehrere Benutzer für die aktuelle Aktion aus.

Aktuell eingeschriebene Rollen

Mit den ausgewählten Benutzern verknüpfte aktuelle Ressourcen.

Andere Rollen

Empfohlene Ressourcen für die ausgewählten Benutzer.

Die Abschnitte "Benutzer" und "Andere Ressourcen" bieten anpassbare Tabellen.

Da das Fenster "MMT-Ressourcen" viele Optionen und große Flexibilität bietet, wird die Prozedur der Aufgabe nach Abschnitten aufgegliedert:

- Die Felder im Abschnitt "Allgemein"
- Die Optionen und Funktionen der Tabelle "Benutzer"
- Die Optionen und Funktionen der Tabelle "Aktuell eingeschriebene Ressourcen"
- Die Optionen und Funktionen der Tabelle "Andere Ressourcen"

Um die Ressourcenzuweisungen Ihres Teams zu verwalten, klicken Sie im Self-Service-Menü auf "Ressourcenzuweisungen meines Teams verwalten". Das Fenster "Ressourcen meines Teams verwalten" wird geöffnet.

Weitere Informationen:

Abschnitt "Allgemein" (Fenster MMT-Ressourcen) (siehe Seite 147)
Benutzertabelle (Fenster MMT-Ressourcen) (siehe Seite 148)
Tabelle "Aktuell eingeschriebene Ressourcen" (Fenster "Meine Rollen verwalten") (siehe Seite 150)
Tabelle "Andere Ressourcen" (Fenster MMT-Ressourcen) (siehe Seite 152)

Abschnitt "Allgemein" (Fenster MMT-Ressourcen)

Der Abschnitt "Allgemein" des Fensters "Ressourcen meines Teams verwalten" enthält die folgenden Felder:

Universum

Wählen Sie das Universum aus, mit dem Sie arbeiten möchten. Die Benutzertabelle und die verfügbaren Ressourcen hängen vom Universum ab.

Geschäftsbereich

Allgemeine Informationen (beschreibend). Diese Information wird im Feld "Beschreibung" des folgenden Self-Service-Genehmigungsstammtickets angezeigt.

Geschäftsprozess

Allgemeine Informationen (beschreibend). Diese Information wird im Feld "Beschreibung" des folgenden Self-Service-Genehmigungsstammtickets angezeigt.

Beschreibung

Geben Sie eine genaue und sinnvolle Beschreibung der Änderungen ein, die sie an den Ressourcen Ihres Teams vornehmen möchten.

Senden

Klicken Sie auf "Senden", um Änderungen anzufragen.

So geben Sie Daten im Abschnitt "Allgemein" der MMT-Ressource ein

1. Wählen Sie ein Universum in der Dropdown-Liste aus.
2. Geben Sie den Geschäftsbereich für die aktuelle Aktion ein.
3. Geben Sie den Geschäftsprozess ein, der mit der aktuellen Aktion verbunden ist.
4. Geben Sie eine Beschreibung ein.

Benutzertabelle (Fenster MMT-Ressourcen)

Die Tabelle "Benutzer" zeigt eine Liste der Benutzer in den Konfigurationsdateien des ausgewählten Universums an. Die Mitglieder Ihres Teams sind mir einem grünen Punkt neben ihrem Namen markiert.

Die Tabelle "Benutzer" bietet die folgenden Optionen:

Hinzufügen

Eine Spalte mit Kontrollkästchen, eines pro Benutzer. Wählen Sie eines oder mehrere aus. Wenn Sie mehrere Benutzer auswählen, werden alle Änderungen, die Sie vornehmen, für alle ausgewählten Benutzer implementiert.

Personen-ID

Klicken Sie auf eine hervorgehobene ID, der in dieser Spalte erscheint, um die entsprechende Benutzerkarte zu öffnen.

Ressourcen abrufen

Bietet eine Tabelle der aktuell eingeschriebenen Ressourcen für die ausgewählten Benutzer.

Anpassen

Ermöglicht es Ihnen, die Spalten festzulegen, die in der Tabelle "Benutzer" angezeigt werden.

Datensätze pro Seite

Wählen Sie die Anzahl an Datensätzen, die in der Tabelle "Benutzer" angezeigt werden.

Benutzer suchen

Öffnet das Filterfenster "Benutzer auswählen", um Sie bei der Suche nach spezifischen Benutzern zu unterstützen.

Wenn Sie die Benutzer ausgewählt haben, die sie jetzt verwalten möchten, könne sie auf "Ressourcen abrufen" klicken, um eine Liste der aktuell mit diesen Benutzern verbundenen Ressourcen zu erhalten.

Hinweis: Wenn die Aktionen, die Sie unternehmen wollen, nicht die aktuell mit dem ausgewählten Benutzer verbundenen eingeschrieben Ressourcen einbeziehen, können Sie die Tabelle "Aktuell eingeschriebene Ressourcen" überspringen und zur Tabelle "Andere Ressourcen" wechseln.

So wählen Sie Benutzer aus der Tabelle "Benutzer" der MMT-Ressourcen aus und rufen deren Rollen ab

1. Wählen Sie einen oder mehrere Benutzer in der Tabelle "Benutzer" aus. Sie können auf "Benutzer suchen" klicken, um das Fenster "Benutzer auswählen" zu öffnen.
2. Auf "Ressourcen abrufen" klicken.

   Die mit dem/n ausgewählten Benutzer(n) verknüpften Ressourcen werden in der Tabelle "Aktuell eingeschriebene Ressourcen" angezeigt. Eine Liste der Ressourcen, die nicht mit dem/n aktuell ausgewählten Benutzer(n) verknüpft sind, wird in der Tabelle "Andere Ressourcen" angezeigt.

   Jetzt können Sie aus folgenden Möglichkeiten auswählen:

   - Die aktuelle Einschreibungsliste verwalten
   - Zusätzliche Ressourcen für die ausgewählten Benutzer hinzufügen.
   - Beide ausführen.

Wenn sie die aktuell eingeschrieben Ressourcen nicht verwalten möchten, fügen Sie den ausgewählten Benutzern Ressourcen hinzu.

Weitere Informationen:

Tabelle "Aktuell eingeschriebene Ressourcen" (Fenster "Meine Rollen verwalten") (siehe Seite 150)
Tabelle "Andere Ressourcen" (Fenster MMT-Ressourcen) (siehe Seite 152)

Tabelle "Aktuell eingeschriebene Ressourcen" (Fenster "Meine Rollen verwalten")

Dieser Abschnitt ermöglicht es Ihnen, die aktuelle Einschreibung von Ressourcen für Ihre ausgewählten Benutzer zu verwalten. Die Optionen, die Ihnen zur Verfügung stehen, hängen davon ab, wie viele Benutzer Sie für die aktuelle Aktion ausgewählt haben.

Wenn nur ein Benutzer ausgewählt ist, klicken Sie auf "Ressourcen abrufen", um eine Liste der mit diesem ausgewählten Benutzer verbundenen Ressourcen zu erhalten.

In diesem Fall ist besteht die einzige Ihnen zur Verfügung stehende Option darin, das Kontrollkästchen "Entfernen" neben der Ressource zu aktivieren und damit den Link zwischen dem Benutzer und der Ressource zu trennen.

Wenn Sie mehr als einen Benutzer auswählen, bietet Ihnen die Tabelle "Aktuell eingeschriebene Ressourcen" eine zusätzliche Spalte: Einschreibung.

Wenn mehrere Benutzer ausgewählt sind, können Sie:

- Das Kontrollkästchen "Entfernen" neben der Ressource aktivieren und damit den Link zwischen dem Benutzer und der ausgewählten Ressource trennen.
- Das Kontrollkästchen "Hinzufügen" neben einer Ressource aktivieren, bei der nur einige der ausgewählten Benutzer eingeschrieben sind und damit alle ausgewählten Benutzer mit der ausgewählten Ressource verknüpfen.

Die Tabelle "Aktuell eingeschriebene Ressourcen" bietet folgende Optionen:

Hinzufügen

Eine Spalte mit Kontrollkästchen, eines pro Ressource. Wählen Sie eines oder mehrere aus. Die Kontrollkästchen neben Ressourcen, die bereits mit allen ausgewählten Benutzern verknüpft sind, sind nicht aktiv.

Entfernen

Eine Spalte mit Kontrollkästchen, eines pro Ressource. Aktivieren Sie eines oder mehrere, um den Link des ausgewählten Benutzers mit den ausgewählten Ressourcen zu entfernen.

Einschreibung

Diese Spalte wird nur dann angezeigt, wenn mehrere Benutzer ausgewählt sind. Zeigt in Zahlen an [Anzahl der eingeschriebenen Benutzer]/[Gesamtanzahl der ausgewählten Benutzer], 2/3 bedeutet zum Beispiel, dass zwei der drei ausgewählten Benutzer bei dieser Ressource eingeschrieben sind. Diese Spalte bietet den Wert auch als prozentualen Wert. Beispiel: 1/3 (33%).

Ressourcenname

Klicken Sie auf einen hervorgehobenen Ressourcennamen, der in dieser Spalte erscheint, um seine Ressourcenkarte zu öffnen.

Je nachdem, welche Aktion Sie ausführen möchten, haben Sie die Aufgabe möglicherweise nach dem Aktivieren der entsprechenden Kontrollkästchen bereits abgeschlossen. In diesem Fall können Sie die Anweisungen in "Andere Ressourcen" ignorieren und Ihre Anfragen mir einem Klick auf "Senden" unten im Fenster "Die Ressourcen meines Teams verwalten" senden.

Um in der Tabelle "Aktuell eingeschriebene Ressourcen" eine Auswahl zu treffen, aktivieren Sie die entsprechenden Kontrollkästchen in der Spalte "Hinzufügen Und/oder Entfernen" der Tabelle "Aktuell eingeschriebene Ressourcen".

Jetzt können Sie aus folgenden Möglichkeiten auswählen:

- Den Prozess hier abbrechen
- Zusätzliche Ressourcen für die ausgewählten Benutzer hinzufügen.

Wenn Sie keine neuen Ressourcen hinzufügen möchten, senden Sie Ihre Anfragen.

Tabelle "Andere Ressourcen" (Fenster MMT-Ressourcen)

Dieser Abschnitt ermöglicht es Ihnen, Ihre(n) ausgewählten Benutzer bei zusätzlichen Ressourcen Ihrer Wahl einzuschreiben. Die Einschreibung an sich erfolgt nach einem Überprüfungsprozess.

Hinweis: Wenn Sie auf "Ressourcen abrufen" im Abschnitt "Benutzer" klicken, wird in der Tabelle "Andere Ressourcen" eine Liste von Ressourcen angezeigt, die nicht mit dem/n aktuell ausgewählten Benutzer(n) verknüpft sind.

Über die Verwaltung der aktuell mit Mitgliedern Ihres Teams verknüpften Ressourcen hinaus können Sie eine Liste der für Ihre ausgewählten Benutzer empfohlenen Ressourcen vom System anfordern. Die Liste der Ressourcen wird im Abschnitt "Andere Ressourcen" angezeigt.

Der Abschnitt "Andere Ressourcen" bietet Ihnen die folgenden Optionen:

Hinzufügen

Eine Spalte mit Kontrollkästchen, eines pro Rolle. Wählen Sie eines oder mehrere aus, um die ausgewählten Benutzer mit zusätzlichen Ressourcen zu verknüpfen.

Ressourcenname 1

Klicken Sie auf einen hervorgehobenen Ressourcennamen, der in dieser Spalte erscheint, um seine Ressourcenkarte zu öffnen.

Anpassen

Ermöglicht es Ihnen, die Spalten festzulegen, die in der Tabelle "Andere Ressourcen" angezeigt werden.

Datensätze pro Seite

Wählen Sie die Anzahl an Datensätzen, die in der Tabelle "Andere Ressourcen" angezeigt werden.

Ressourcen suchen

Öffnet das Filterfenster "Ressourcen auswählen", um Sie bei der Suche nach spezifischen Ressourcen zu unterstützen.

Testen der Compliance

Überprüft, ob die in der Tabelle "Andere Ressourcen" vorgenommene Auswahl bestehenden Richtlinien und BPRs (Geschäftsprozessregeln) entspricht.

Ressourcen vorschlagen

Bietet eine Liste möglicher Ressourcen auf der Basis der CA RCM-Mustererkennungs-Technologie.

Diese Tabelle bietet Ihnen mehrere Optionen:

- Sie können manuell eine oder mehrere Ressourcen auswählen, die Sie mit den ausgewählten Benutzern verknüpfen möchten.
- Sie können die Option "Ressourcen suchen". verwenden, um spezifische Rollen zu suchen, und dann eine Auswahl in der gefilterten Ressourcenliste treffen.
- Sie können auf "Ressourcen vorschlagen" klicken und die in dieser Funktion angebotenen Informationen nutzen, um Ressourcen mit den ausgewählten Benutzern zu verknüpfen.

Nachdem Sie Ihre Auswahl getroffen haben, können Sie die Übereinstimmung Ihrer Auswahl mit bestehenden BPRs und Richtlinien überprüfen.

Sie können entscheiden, ob Sie die Anfrage trotz der aufgeführten Nichtübereinstimmungen ausführen, oder ob Sie Ihre Auswahl ändern.

Wichtig! Bitte bedenken Sie bei der Auswahl mehrerer Benutzer, dass jede ressourcenbezogene Auswahl auf alle Benutzer gleich angewendet wird. Wenn Sie die Auswahl der Benutzer ändern, klicken Sie erneut auf "Ressourcen abrufen".

So verknüpfen Sie Ressourcen mit den ausgewählten Benutzern

1. Im Fenster "Die Ressourcen meines Teams verwalten" scrollen Sie nach unter zur Tabelle "Andere Ressourcen".
2. (Optional) Klicken Sie auf "Ressourcen suchen", um zum Filterfenster "Ressource auswählen" zu gelangen.
3. (Optional) Klicken Sie auf "Ressourcen vorschlagen", um die Vorschläge des CA RCM-Portals anzuzeigen.
4. Wählen Sie eine oder mehrere Ressourcen aus, die mit den ausgewählten Benutzern verknüpft werden.
5. (Optional) Klicken Sie auf "Compliance testen", um Ihre Auswahl auf mögliche Verletzungen hin zu überprüfen.

   Das Fenster "Verletzungen" wird in einem separaten Browserfenster geöffnet. Klicken Sie auf X, um das Fenster "Verletzungen" zu schließen.
6. Klicken Sie auf "Senden".

   Das Fenster "Anfrage" wird angezeigt.

Weitere Informationen:

Wie CA RCM Entitäten vorschlägt (siehe Seite 128)
Testen der Compliance (siehe Seite 127)

Meine Ressourcen verwalten

Als Benutzer müssen Sie möglicherweise aufgrund von Unternehmensänderungen, Änderungen bei Ressourcen oder infolge eines Auditprozesses eine Aktualisierung Ihrer Ressourcen anfordern. Das Fenster "Meine Ressourcen verwalten" ermöglicht es Ihnen, Ihre Ressourcen zu verwalten, indem Sie eine Anfrage für das Hinzufügen neuer Ressourcen erstellen oder bestehende Ressourcen löschen.

Das Fenster ist in drei Abschnitte unterteilt:

Allgemein

Bietet beschreibende Informationen zur laufenden Aktion.

Aktuell eingeschriebene Ressourcen

Mit den ausgewählten Benutzern verknüpfte aktuelle Ressourcen.

Andere Ressourcen

Eine Liste verfügbarer Ressourcen.

Der Abschnitt "Andere Ressourcen" zeigt eine anpassbare Tabelle an:

Da das Fenster "Meine Ressourcen verwalten" viele Optionen und große Flexibilität bietet, werden die Prozeduren nach Abschnitten aufgegliedert:

- Die Felder im Abschnitt "Allgemein"
- Die Optionen und Funktionen der Tabelle "Aktuell eingeschriebene Ressourcen"
- Die Optionen und Funktionen der Tabelle "Andere Ressourcen"

Um Ihre Ressourcen zu verwalten, klicken Sie im Self-Service-Menü auf "Meine Ressourcenzuweisungen verwalten". Das Fenster "Meine Ressourcen verwalten" wird geöffnet.

Weitere Informationen:

Abschnitt "Allgemein" (Fenster "Meine Ressourcen verwalten") (siehe Seite 156)
Tabelle "Aktuell eingeschriebene Ressourcen" (Fenster "Meine Ressourcen verwalten") (siehe Seite 157)
Tabelle "Andere Ressourcen" (Fenster "Meine Ressourcen verwalten") (siehe Seite 158)

Abschnitt "Allgemein" (Fenster "Meine Ressourcen verwalten")

Der Abschnitt "Allgemein" des Fensters "Meine Ressourcen verwalten" enthält die folgenden Felder:

Universum

Wählen Sie das Universum aus, mit dem Sie arbeiten möchten. Die Benutzertabelle und die verfügbaren Ressourcen hängen vom Universum ab.

Geschäftsbereich

Allgemeine Informationen (beschreibend). Diese Information wird im Feld "Beschreibung" des folgenden Self-Service-Genehmigungsstammtickets angezeigt.

Geschäftsprozess

Allgemeine Informationen (beschreibend). Diese Information wird im Feld "Beschreibung" des folgenden Self-Service-Genehmigungsstammtickets angezeigt.

Beschreibung

Geben Sie eine genaue und sinnvolle Beschreibung der Änderungen ein, die sie an Ihren Ressourcen vornehmen möchten.

Senden

Klicken Sie auf "Senden", um Änderungen anzufragen.

So geben Sie Daten im Abschnitt "Allgemein" von "Meine Ressourcen verwalten" ein

1. Wählen Sie ein Universum in der Dropdown-Liste aus.

   Die Tabelle "Aktuell eingeschriebene Ressourcen" und die Tabelle "Andere Ressourcen" zeigen Ressourcen an, die der Konfiguration des ausgewählten Universums angehören.

2. Geben Sie den Geschäftsbereich für die aktuelle Aktion ein.
3. Geben Sie den Geschäftsprozess ein, der mit der aktuellen Aktion verbunden ist.
4. Geben Sie eine Beschreibung ein.

Hinweis: Wenn die Aktionen, die Sie unternehmen wollen, nicht Ihre aktuell eingeschrieben Ressourcen einbeziehen, können Sie die Tabelle "Aktuell eingeschriebene Ressourcen" überspringen und zur Tabelle "Andere Rollen" wechseln.

Wenn sie die aktuell eingeschrieben Ressourcen nicht verwalten möchten, fügen Sie den ausgewählten Benutzern Ressourcen hinzu.

Tabelle "Aktuell eingeschriebene Ressourcen" (Fenster "Meine Ressourcen verwalten")

Dieser Abschnitt ermöglicht es Ihnen, Ihre aktuell eingeschriebenen Ressourcen zu verwalten. Als Sie das Universum ausgewählt haben, hat Ihnen das Portal CA RCM eine Liste Ihrer aktuellen Ressourcen innerhalb der Konfiguration des Universums zur Verfügung gestellt.

In diesem Fall ist besteht die einzige Ihnen zur Verfügung stehende Option darin, das Kontrollkästchen "Entfernen" neben der Ressource zu aktivieren und damit Ihren Link mit der Ressource zu trennen.

Die Tabelle "Aktuell eingeschriebene Ressourcen" bietet folgende Optionen:

Entfernen

Eine Spalte mit Kontrollkästchen, eines pro Benutzer. Aktivieren Sie eines oder mehrere, um den Link des ausgewählten Benutzers mit den ausgewählten Ressourcen zu entfernen.

Ressourcenname 1

Klicken Sie auf einen hervorgehobenen Ressourcennamen, der in dieser Spalte erscheint, um seine Ressourcenkarte zu öffnen.

Je nachdem, welche Aktion Sie ausführen möchten, haben Sie die Aufgabe möglicherweise nach dem Aktivieren der entsprechenden Kontrollkästchen bereits abgeschlossen. In diesem Fall können Sie die Anweisungen in "Andere Ressourcen" ignorieren und Ihre Anfragen mir einem Klick auf "Senden" unten im Fenster "Meine Ressourcen verwalten" senden.

Um in der Tabelle "Aktuell eingeschriebene Ressourcen" eine Auswahl zu treffen, aktivieren Sie die entsprechenden Kontrollkästchen in der Spalte "Entfernen" der Tabelle "Aktuell eingeschriebene Ressourcen".

Jetzt können Sie aus folgenden Möglichkeiten auswählen:

- Den Prozess hier abbrechen
- Ressourcen hinzufügen

Wenn Sie keine neuen Ressourcen hinzufügen möchten, senden Sie Ihre Anfragen.

Tabelle "Andere Ressourcen" (Fenster "Meine Ressourcen verwalten")

Dieser Abschnitt ermöglicht es Ihnen, sich bei zusätzlichen Ressourcen Ihrer Wahl einzuschreiben. Die Einschreibung an sich erfolgt nach einem Überprüfungsprozess.

Über die Verwaltung der Ressourcen, mit denen Sie derzeit verbunden sind, hinaus können Sie eine Liste der für Sie empfohlenen Ressourcen vom System anfordern. Die Liste der Ressourcen wird im Abschnitt "Andere Ressourcen" angezeigt.

Der Abschnitt "Andere Ressourcen" bietet Ihnen die folgenden Optionen:

Hinzufügen

Eine Spalte mit Kontrollkästchen, eines pro Ressource. Wählen Sie eines oder mehrere aus.

Ressourcenname 1

Klicken Sie auf einen hervorgehobenen Ressourcennamen, der in dieser Spalte erscheint, um seine Ressourcenkarte zu öffnen.

Anpassen

Ermöglicht es Ihnen, die Spalten festzulegen, die in der Tabelle "Andere Ressourcen" angezeigt werden.

Datensätze pro Seite

Wählen Sie die Anzahl an Datensätzen, die in der Tabelle "Andere Ressourcen" angezeigt werden.

Ressourcen suchen

Öffnet das Filterfenster "Ressource auswählen", um Sie bei der Suche nach spezifischen Ressourcen zu unterstützen.

Testen der Compliance

Überprüft, ob die in der Tabelle "Andere Ressourcen" vorgenommene Auswahl bestehenden Richtlinien und BPRs (Geschäftsprozessregeln) entspricht.

Ressourcen vorschlagen

Bietet eine Liste möglicher Ressourcen auf der Basis der CA RCM-Mustererkennungs-Technologie.

Diese Tabelle bietet Ihnen mehrere Optionen:

- Sie können manuell eine oder mehrere Ressourcen auswählen, bei denen Sie sich einschreiben möchten.
- Sie können die Option "Ressourcen suchen". verwenden, um spezifische Ressourcen zu suchen und dann eine Auswahl in der gefilterten Ressourcenliste treffen.
- Sie können auf "Ressourcen vorschlagen" klicken und die in dieser Funktion angebotenen Informationen nutzen, um Ressourcen zu finden, bei denen Sie sich einschreiben sollten.

Nachdem Sie Ihre Auswahl getroffen haben, können Sie die Übereinstimmung Ihrer Auswahl mit bestehenden BPRs und Richtlinien überprüfen.

Sie können entscheiden, ob Sie die Anfrage trotz Nichtübereinstimmung ausführen, oder ob Sie Ihre Auswahl ändern.

So verknüpfen Sie mit zusätzlichen Ressourcen

1. Im Fenster "Meine Ressourcen verwalten" scrollen Sie nach unter zur Tabelle "Andere Ressourcen".
2. (Optional) Klicken Sie auf "Ressourcen suchen", um zum Filterfenster "Ressource auswählen" zu gelangen.
3. (Optional) Klicken Sie auf "Ressourcen vorschlagen", um die Vorschläge des CA RCM-Portals anzuzeigen.
4. Wählen Sie eine oder mehrere Ressourcen aus, die mit den ausgewählten Benutzern verknüpft werden.
5. (Optional) Klicken Sie auf "Compliance testen", um Ihre Auswahl auf mögliche Verletzungen hin zu überprüfen.

   Das Fenster "Verletzungen" wird in einem separaten Browserfenster geöffnet. Klicken Sie auf , um das Fenster "Verletzungen" zu schließen.
6. Klicken Sie auf "Senden".

   Das Fenster "Anfrage" wird angezeigt.

Weitere Informationen:

Testen der Compliance (siehe Seite 127)
Wie CA RCM Entitäten vorschlägt (siehe Seite 128)
Einführung in die Anfragentabellen (siehe Seite 169)

Neue Rolle definieren

Zusätzlich zu der von CA RCM generierten Rollenhierarchie, können Sie neue Rollen definieren.

Weitere Informationen:

Fenster "Neue Rollendefinition anfordern" (siehe Seite 161)
Definitionen für Rollennamen [Neuer Rollenname] (siehe Seite 165)

Fenster "Neue Rollendefinition anfordern"

Der erste Schritt in der Definition einer neuen Rolle ist die Definition ihrer Charakteristiken und allgemeinen Definitionen. Für eine neue Rolle mit dem Namen "Sicherheitsbeauftragter", zum Beispiel, müssen Sie den Rollennamen, die unternehmensinternen Definitionen und die Regeln angeben, die diese Rolle regeln.

Das Fenster "Neue Rollendefinition anfordern" ist in zwei Abschnitte unterteilt:

- Aufgabendefinitionen
- Rollendefinitionen

Der Bereich "Aufgabendefinitionen" umfasst die folgenden Felder:

Universum

Definiert das Universum, mit dem Sie arbeiten möchten. Die neue Rolle wird mit dieser Universumskonfiguration asoziiert. Die Benutzertabelle und die verfügbaren Ressourcen, die im Fenster "Definitionen für Rollennamen [Neue Rolle]" angegeben werden, hängen vom Universum ab.

Geschäftsbereich

Allgemeine Informationen (beschreibend). Diese Information erscheint im Feld "Beschreibung" des folgenden Self-Service-Genehmigungsstamm-Tickets.

Geschäftsprozess

Allgemeine Informationen (beschreibend). Diese Information erscheint im Feld "Beschreibung" des folgenden Self-Service-Genehmigungsstamm-Tickets.

Anfragebeschreibung

Bietet eine klare und aussagekräftige Beschreibung der neuen Rolle und ihres Zwecks.

Der Bereich "Rollendefinitionen" umfasst die folgenden Felder:

Rollenname

Der Name der neuen Rolle (präzise und beschreibend).

Beschreibung

Beschreibt die neue Rolle.

Eigentümer

Definiert den Benutzer im Zieluniversum, der Eigentümer der neuen Rolle ist. Standardmäßig sind Sie der Eigentümer der Rolle, die Sie anfordern. Lassen Sie dieses Feld leer, um Ihrer Rolle als Eigentümer zu akzeptieren, oder geben Sie einen anderen Benutzer im Universum an.

Typ

Gibt den Rollentyp an (verwenden Sie AutoComplete).

Organisation

Gibt den Namen der Hauptorganisation an (verwenden Sie AutoComplete).

Organisation 2

Gibt den Namen der sekundären Organisation an (verwenden Sie AutoComplete).

Organisation 3

Gibt den Namen der tertiären Organisation an (verwenden Sie AutoComplete).

Regel

(Optional) Gibt eine Regel für die neue Rolle an. Sie können die Funktion "Regel hinzufügen" verwenden, um eine Regel zu konstruieren.

So definieren Sie eine neue Rolle:

1. Klicken sie im Self-Service-Menü auf "Neue Rollendefinition anfordern".

   Das Fenster "Neue Rollendefinition anfordern" wird geöffnet.

2. Wählen Sie ein Universum in der Dropdown-Liste aus.

   Die neu definierte Rolle wird mit der Konfiguration assoziiert, die diesem Universum angehört. Die mit dieser Rolle zu verknüpfenden Benutzer und Ressourcen werden aus dieser Universumskonfiguration entnommen.

3. Geben Sie den Geschäftsbereich für die aktuelle Aktion ein.
4. Geben Sie den Geschäftsprozess ein, der mit der aktuellen Aktion verbunden ist.
5. Geben Sie die Beschreibung der Anfrage ein.
6. Rollennamen eingeben.
7. Geben Sie die Beschreibung der neuen Rolle ein.
8. Geben Sie die Eigentümer-ID ein. (Optional) Klicken Sie auf "Suchen", um auf das Filterfenster "Benutzer suchen" zuzugreifen.
9. Wählen Sie einen Benutzer aus der mit Ihrem Filter generierten Benutzerliste aus. Klicken Sie auf "OK".
10. Geben Sie einen Typ an (verwenden Sie AutoComplete).
11. Geben Sie einen Organisationsnamen an (verwenden Sie AutoComplete).
12. Geben Sie einen Namen für die Organisation 2 an (verwenden Sie AutoComplete).
13. Geben Sie einen Namen für die Organisation 3 an (verwenden Sie AutoComplete).
14. Eine Regel erstellen Klicken Sie auf "Regel hinzufügen", um Hilfe bei der Konstruktion einer Regel zu erhalten.
15. Klicken Sie auf "Next". Das Fenster "Definitionen für Rollennamen" [Rollenname] wird angezeigt.

Weitere Informationen:

Eine Regel konstruieren (siehe Seite 164)
Definitionen für Rollennamen [Neuer Rollenname] (siehe Seite 165)

Eine Regel konstruieren

Das Portal CA RCM bietet Ihnen das Hilfsprogramm "Regel hinzufügen", um Ihnen bei der Konstruktion einer Regel für die neue Rolle, die Sie anfordern, zu unterstützen.

Dieses Fenster verfügt über die folgenden Textfelder und Funktionen:

Feld

Verwenden Sie AutoComplete, um einen Namen für das Feld auszuwählen.

Wert

Geben Sie einen Wert ein oder verwenden Sie AutoComplete, um einen geeigneten Wert anzugeben.

Hinzufügen

Ermöglicht es Ihnen, eine weitere Beschränkung zur Rolle hinzuzufügen.

Entfernen

Entfernt die letzte hinzugefügte Beschränkung.

Abbrechen

Bricht die Regelkonstruktion ab.

Hinweis: Das Hinzufügen einer Regel ist optional. Nicht jede Rolle muss regelbasiert sein.

So konstruieren Sie eine Regel

1. Klicken Sie auf "Regel hinzufügen" im Fenster "Neue Rollendefinition anfordern".

   Das Fenster "Rollenkonstruktion" wird geöffnet.

2. Geben Sie einen Feldnamen ein.
3. Wert eingeben
4. (Optional) Klicken Sie auf "Hinzufügen", um zusätzliche Beschränkungen hinzuzufügen.
5. Wiederholen Sie Schritt 2 bis 4 so oft wie nötig.
6. Klicken Sie auf OK.

   Die konstruierte Regel erscheint im Regel-Textfeld im Fenster "Neue Rollendefinition anfordern".

Definitionen für Rollennamen [Neuer Rollenname]

Nachdem Sie jetzt die neue Rolle angefordert haben, können Sie damit beginnen, dieser neu konstruierten Rolle Benutzer und Ressourcen zuzuweisen. Rollen können in einer hierarchischen Beziehung mit Benutzern, Ressourcen und anderen Rollen in über- oder untergeordneter Position verknüpft werden. Das Fenster "Definitionen für Rollennamen [Neuer Rollenname]" bietet Ihnen die Möglichkeit, schnell und einfach auszuwählen, welche Links Ihre neue Rolle haben wird.

Wenn Sie Ihre Auswahl abgeschlossen haben, können Sie diese auf Verletzungen hin prüfen. Wenn Sie mit dem Ergebnis zufrieden sind, klicken Sie auf die Schaltfläche "Senden", die sich zwischen den Entitätentabellen befindet, um eine neue Rollendefinition anzufordern. Die Anfrage kann von Ihnen überprüft werden, und wenn Sie keine Korrekturen vornehmen möchten, klicken Sie auf "Senden" unterhalb der Anfragetabelle und generieren Sie die zur Bestätigung der erstellten Rollendefinitionen nötigen Genehmigungsvorgangstickets.

Hinweis: Die in der Benutzertabelle mit einem grünen Punkt neben ihrem Namen markierten Benutzer sind Benutzer, die Ihnen gegenüber "accountable" sind (RACI).

Dieses Fenster ist in drei Abschnitte unterteilt:

- Ressourcen
- Benutzer
- Rollenhierarchie - kann in zwei Bereiche erweitert werden:
- Übergeordnete Rollen
- Untergeordnete Rollen

Die Rollenhierarchie entwickelt sich aus Rollenstrukturen, die in vielen Unternehmenssystemen präsent sind. Eine Identity Manager-Anwendung kann zum Beispiel zwei Rollenebenen haben: Bereitstellungsrolle und Bereitstellungsrichtlinie. Benutzer werden immer mit einer Bereitstellungsrolle verknüpft, die mit einer spezifischen Bereitstellungsrichtlinie verknüpft ist. Diese hierarchische Struktur wird bei Import/Export beibehalten. Wenn eine neue Rolle generiert wird, ist es wichtig, zu wissen, ob es Systemrollen gibt, die spezifische hierarchische Verbindungen zwischen Rollen erfordern.

Jeder Abschnitt enthält eine anpassbare Entitätentabelle, die alle relevanten Entitäten auflistet. Um Sie bei Ihrer Auswahl zu unterstützen, sind die folgenden Funktionen verfügbar:

Entitäten suchen

Bietet ein Filterfenster.

Entitäten vorschlagen

Bietet empfohlene Benutzer für ausgewählte Ressourcen oder empfohlene Ressourcen für ausgewählte Benutzer. Dieser Dienst ist in den Rollenhierarchietabellen nicht verfügbar.

Hervorgehobene Spalte

In jeder anpassbaren Tabelle gibt es eine vordefinierte Spalte, die hervorgehoben ist. Klicken Sie auf den Namen der Entität, um auf ihre Datenkarte zugreifen zu können.

Anpassen

Bietet die Möglichkeit, die Felder auszuwählen, die in der angegebenen Tabelle erscheinen.

Datensätze pro Seite

Festlegen der Anzahl an Datensätzen pro Seite

Testen der Compliance

Prüft Ihre Auswahl auf Verletzungen hin.

Wenn Sie den Dienst "Entitäten vorschlagen" sowohl auf Benutzer als auch auf Ressourcen anwenden, sehen Sie Daten zur Einschreibung von Benutzern und Ressourcen.

So weisen Sie der neuen Rolle Benutzer, Ressourcen und Rollenhierarchie zu

1. Wählen Sie Benutzer-, Ressourcen- und/oder Rollenhierarchie-Entitäten aus. Verwenden Sie bei Bedarf den Entitäten-Filter und das Hilfsprogramm "Entitäten vorschlagen".
2. Klicken Sie auf "Compliance testen", um Ihre Auswahl auf Verletzungen hin zu prüfen.
3. Klicken Sie auf "Senden", um die neue Rollendefinitionsanfrage zu senden.

   Das Fenster "Anfrage" wird angezeigt. Das Fenster "Anfrage" bietet die Attribute und Links der neuen Rolle.
4. Klicken Sie auf "Zurück", um die Daten zu ändern.
5. Klicken Sie auf "Senden", um die Anfrage, eine neue Rolle zu generieren, weiterzuleiten.

Weitere Informationen:

Fenster "Neue Rollendefinition anfordern" (siehe Seite 161)
Wie CA RCM Entitäten vorschlägt (siehe Seite 128)
Testen der Compliance (siehe Seite 127)
Einführung in die Anfragentabellen (siehe Seite 169)

Rollendefinitionen aktualisieren

Das CA RCM-Portal ermöglicht es Ihnen, Rollenattribute und Links kurzfristig zu definieren.

Wenn die Aktualisierung einer bestehenden Rolle notwendig wird, sei es nach einem Audit oder im Lebenszyklus eines Unternehmens, können Sie dies schnell und unkompliziert tun. Die Prozedur umfasst das Suchen der Rolle innerhalb eines spezifischen Universums und das Folgen der Prozedur, die in "Neue Rolle definieren" beschrieben ist, mit dem Unterschied, dass die Felder bereits ausgefüllt, die Attribute definiert und die Links aufgelistet sind; Ihr Ziel ist es nun, diese Auswahl zu bearbeiten, um sie den neuen Bedürfnissen Ihrer Körperschaft anzupassen.

Im Fenster "Rollenaktualisierung anfordern" müssen Sie ein Universum auswählen. Die Auswahl des Universums öffnet das Fenster "Rolle auswählen".

Es handelt sich hierbei um ein Suchfenster mit eingebauten Filtern und einer erweiterten Suchfunktion auf RACI-Basis.

Hinweis: Die Modellkonfiguration des Universums ist in der oberen rechten Ecke des Fensters "Rolle auswählen" aufgelistet.

Sobald Sie erfolgreich ein Suchmuster konstruiert haben, wird in der Tabelle "Rollen" eine Liste von Rollen angezeigt.

So aktualisieren Sie eine bestehende Rolle

1. Klicken sie im Self-Service-Menü auf "Änderungen einer Rollendefinition anfordern".

   Das Fenster "Rollenaktualisierung anfordern" wird geöffnet.

   Wählen Sie ein Universum in der Dropdown-Liste aus.

2. Klicken Sie auf OK.
3. Das Fenster "Rolle auswählen" wird geöffnet.
4. Filtern Sie die Datentabelle, um ein Suchmuster zu erstellen.
5. (Optional) Sie können die erweiterte Suchfunktion auf RACI-Basis verwenden, um zusätzliche Beschränkungen der Suche mit einzuschließen.
6. Klicken Sie auf "Suchen".

   Eine Liste von Rollen wird in der anpassbaren Rollentabelle angezeigt.

7. Aktivieren Sie das Kontrollkästchen der Rolle, die Sie aktualisieren möchten.
8. Klicken Sie auf OK.

   Das Fenster "Rollenaktualisierung anfordern" wird geöffnet.

Weitere Informationen:

Neue Rolle definieren (siehe Seite 161)
Fenster "Neue Rollendefinition anfordern" (siehe Seite 161)
Definitionen für Rollennamen [Neuer Rollenname] (siehe Seite 165)

Einführung in die Anfragentabellen

Jede Self-Service-Aufgabe erfordert, eine Anfrage zu stellen, um die über das Aufgabenfenster erstellte Änderungen auszuführen. Wenn Sie im ausgewählten Fenster "Self-Service" Ihre Auswahl getroffen haben und anschließend auf "Senden" klicken, wird das Fenster "Anfrage" angezeigt. Dieses Fenster fasst alle Anfragen zusammen, die Sie bei der Ausführung der Self-Service-Aufgabe gestellt haben.

Je nach Self-Service-Aufgabe kann das Fenster "Anfrage" auch zusätzliche Informationen enthalten. Zum Beispiel, wenn Sie eine neue Rolle erstellen, werden im Fenster "Anfrage" auch Daten zu den Attributen der neuen Rolle angezeigt.

Die in diesem Fenster angezeigten Spalten der Tabelle "Links" hängen von der Art der Self-Service-Anfrage ab, die Sie bearbeiten. Hervorgehobene Daten bieten Ihnen Zugriff auf relevante Entitätenkarten und weitere Informationen. Diese Informationen bestehen immer aus den folgenden zwei Spalten:

Anfrage

Gibt die Art der Self-Service-Anfrage an. Die Optionen sind "Entfernen" oder "Hinzufügen".

Verletzungen

Gibt die Nummer der Verletzungen an, die mit der bestimmten Anfrage verknüpft sind. Klicken Sie auf die Nummer, um weitere Details anzuzeigen.

Das CA RCM-Portal bietet Ihnen hier zwei Funktionen:

Zurück

Sie kehren zum vorhergehenden Fenster zurück und können Ihre Auswahl bearbeiten.

Senden

Ihre Anfrage wird zur Bearbeitung an CA RCM gesendet. Die Statusanzeige "Tickets werden generiert" wird angezeigt.

Im Fall von Self-Service-Bereitstellungsaufgaben und wenn keine Fehler gefunden werden, wird eine Self-Service-Ticketstrukturansicht erstellt und in Ihren Posteingang gestellt. Für jede Anfrage, die in der Tabelle "Anfrage" aufgelistet ist, wird eine Verzweigung in der Self-Service-Ticketstrukturansicht erstellt.

Wenn Sie eine neue Rolle erstellen oder eine bereits vorhandene aktualisieren, werden je nach Bedarf Tickets erstellt.

1. (Optional) Klicken Sie auf "Zurück", um zum vorherigen Fenster zu gelangen und Ihre Auswahl abzuändern.
2. Klicken Sie auf "Senden", um die Self-Service-Anfragetickets zu erstellen. Das Fenster "Anfragen gesendet" wird angezeigt.

Im Fenster "Anfragen gesendet" werden die neuen Ticket-IDs aufgelistet (die ID des Stammtickets des Ticketeigentümers). Sie können die neue Ticketstrukturansicht im Posteingang anzeigen.

Weitere Informationen:

Self-Service-Aufgaben ausführen (siehe Seite 125)

Kapitel 9: Entitäten-Browser

Das Fenster "Entitäten-Browser" zeigt Details einer Konfiguration an.

Im Entitäten-Browser werden anfänglich die folgenden Felder angezeigt:

Universum

Gibt das Universum an, aus dem Sie eine Konfiguration auswählen. Wählen Sie die Option "Alle", um alle Konfigurationen der Datenbank anzuzeigen.

Konfiguration

Gibt die Konfiguration an, die Sie durchsuchen möchten.

Verwenden Sie diese Felder, um eine Konfiguration auszuwählen. Die folgende Registerkarte wird angezeigt:

Benutzer

Zeigt eine Tabelle von Benutzern in der Konfiguration sowie grundlegende Attributwerte. Sie können die Tabelle durch das Hinzufügen zusätzlicher Attributspalten anpassen.

Klicken Sie auf einen Benutzer, um die Details anzuzeigen (siehe Seite 173)

Rollen

Zeigt eine Liste der Rollen in der Konfiguration sowie grundlegende Attributwerte. Sie können die Tabelle durch das Hinzufügen zusätzlicher Attributspalten anpassen.

Klicken Sie auf eine Rolle, um die Details anzuzeigen (siehe Seite 173)

Ressourcen

Zeigt eine Liste der Ressourcen in der Konfiguration sowie grundlegende Attributwerte. Sie können die Tabelle durch das Hinzufügen zusätzlicher Attributspalten anpassen.

Klicken Sie auf eine Ressource, um die Details anzuzeigen (siehe Seite 173)

Statistiken

Zeigt die Anzahl an Entitäten und Links in der Konfiguration an.

Organisationsdiagramm

Zeigt eine konfigurierbare Struktur (siehe Seite 174) der Benutzer- und Managerhierarchie der Konfiguration an.

Dieses Kapitel enthält folgende Themen:

Benutzer-, Rollen- und Ressourcen-Details

Wenn Sie auf Benutzer, Rolle, Ressource oder Konto im Entitäten-Browser klicken, werden in einem Popupfenster Details für jene Entität angezeigt. Das Fenster kann je nach Typ der überprüften Entität die folgenden Registerkarten enthalten:

Benutzer

Zeigt die Benutzer an, die mit der Entität verknüpft sind.

Rollen

Zeigt die Rollen an, die mit der Entität verknüpft sind.

Unterrollen

Zeigt die untergeordneten Rollen der Rolle an.

Übergeordnete Rollen

Zeigt die übergeordneten Rollen der Rolle an.

Ressourcen

Zeigt die Ressourcen an, die mit der Entität verknüpft sind. Wenn das Zieluniversum Nutzungsdaten einer CA Enterprise Log Manager-Instanz enthält, können Sie in der Nutzungsansicht angeben, dass die Nutzungsdaten in dieser Registerkarte angezeigt werden.

Konten

Zeigt die Benutzerkonten auf externen Endpunkten, die mit der Entität verknüpft sind. Diese Registerkarte wird nur angezeigt, wenn das Zieluniversum Kontokonfigurationen enthält.

Genehmigungen

Zeigt die Genehmigungsaufgaben des Benutzers in gegenwärtig aktiven Kampagnen an.

RACI

Zeigt die Benutzer, die mit der Entität durch RACI-Analyse der Konfiguration verknüpft sind.

Ändern des Organisationsdiagramms

Die Registerkarte "Organisationsdiagramm" des Entitäten-Browsers zeigt die Benutzer der Zielkonfiguration in einer klickbaren Struktur an. Jede Ebene der Struktur gruppiert Benutzer, basierend auf dem Wert des Benutzerattributs in der Zielkonfiguration.

Sie können die Strukturebenen nach Wunsch konfigurieren, um Benutzer in verschiedenen Weisen anzuzeigen. Zum Beispiel können Sie eine Struktur erstellen, die die geografische Verteilung der Benutzer zeigt. Sie können auch eine Struktur erstellen, die die Verwaltungsstruktur der Organisation zeigt.

Hinweis: Wenn Sie das Organisationsdiagramm ändern, verändern Sie nur die Struktur der Anzeige der Benutzer. Sie verändern damit keine Benutzerdaten in der Konfiguration.

So ändern Sie Organisationsdiagramme

1. Klicken Sie im Entitäten-Browser auf die Registerkarte "Organisationsdiagramm".
2. Geben Sie im Bereich "Felder auswählen" der Registerkarte, in der Dropdown-Liste auf Ebene 1, das Benutzerattribut an, das die obere Ebene der Struktur bestimmt.
3. Geben Sie das Benutzerattribut in der Dropdown-Liste auf Ebene 2 an, das die nächste Ebene der Struktur bestimmt.
4. Geben Sie weitere Ebenen der Struktur an:
   - Um weitere Ebenen hinzuzufügen, klicken Sie in der Struktur auf das Plus-Symbol der untersten Ebene.

     Eine neue Dropdown-Liste wird angezeigt.
   - Um eine Ebene zu löschen, klicken Sie auf das Minussymbol neben der entsprechenden Ebene.

     Die Dropdown-Liste wird entfernt und die darunterliegenden Ebenen werden neu nummeriert.
5. Klicken Sie auf "Organisationsdiagramm aktualisieren".

   Die Struktur spiegelt nun Ihre Angaben wieder.

Kapitel 10: Generieren von Berichten

Dieses Kapitel enthält folgende Themen:

Wie man Berichte generiert

Berichte stellen benutzerdefinierte Ansichten von rollenbasierten Konfigurationen zur Verfügung, die Sie in CA RCM erstellen. Sie können Berichte generieren, um das Folgende auszuführen:

- Um den Import-/Exportfortschritt, das Rollenmanagement oder die Zertifizierungskampagnen zu verfolgen.
- Um Rollenhierarchien und Benutzer-/Ressourcenzuweisungen im Detail zu analysieren.
- Um Informationen der Managementebene zu rollenbasierten Zugangskontroll- und Compliance-Aktivitäten zu teilen.

CA RCM stellt eine Reihe von vordefinierten Berichtstypen zur Verfügung, die durch das Angeben von Filter-, Sortier- und Schwellenwertparameter benutzerdefiniert werden können.

Folgende Tabelle beschreibt die Schritte zur Generierung eines Berichts in CA RCM:

Schritt	Weitere Informationen finden Sie unter...
1. Wählen Sie einen auszuführenden Bericht.	Berichtstypen (siehe Seite 176)
2. Wählen Sie Datendateien, geben Sie Benutzerdefinitionsparameter an und generieren Sie den Bericht.	Parameter und Filter für die Berichtgenerierung (siehe Seite 177)

Schritt	Weitere Informationen finden Sie unter...
3. Den Bericht in Ihrem Browser ansehen	Zeigen Sie de Berichtsindex an (siehe Seite 180)und verändern Sie Berichtparameter. (siehe Seite 181)
4. Exportieren Sie den Bericht zu einer Datei oder drucken Sie ihn aus.	Exportieren Sie einen Bericht zu einer Datei (siehe Seite 181)oder drucken Sie einen Bericht aus. (siehe Seite 182)

Berichtstypen

Auf Berichte kann über den Menüpunkt "Berichte" im Hauptmenü des CA RCM-Portals zugegriffen werden.

Berichte sind in die folgenden Kategorien gruppiert:

- Konfigurationsberichte - detaillierte Listen von Benutzern, Ressourcen oder Rollen und deren Links zu anderen Entitäten. Diese Berichte ermöglichen es Managern, die den Benutzern oder Ressourcen in ihrem Verantwortungsbereich zugeteilten Berechtigungen im Detail zu prüfen.
- Qualitätsmanagement für Berechtigungen - grafische Darstellungen der geläufigsten, wichtigsten, musterbasierten analytischen Metriken der Konfiguration (vergleichbar mit denen, die in der Auditphase des Rollenmanagements verwendet werden). Diese Berichte geben einen schnellen visuellen Überblick darüber, wie gut die aktuelle Rollenhierarchie Benutzungsmustern entspricht und welcher Anteil der Benutzer verdächtige Zugriffsmuster hat.
- Rollenmanagement - Berichte, die verwendet werden, um die Rollenhierarchie zu analysieren und "Vorher/nachher"- und "Was wenn ...?"-Vergleiche verschiedener Konfigurationen auszuführen.
- Richtlinienmanagement - Berichte, die verwendet werden, um die Verwendung von Geschäftsprozessregeln (Business Process Rules, BPRs) zu überprüfen.
- Kampagnen - Berichte, die verwendet werden, um den Fortschritt der Zertifizierungskampagne zu verfolgen und im Verlauf einer Kampagne vorgenommene Änderungen zusammenzufassen.

Parameter und Filter für die Berichtgenerierung

Um einen Bericht zu erstellen, müssen Sie die Konfigurationsdatei oder das Universum angeben, auf die sich Ihr Bericht beziehen soll. Sie müssen für einige Berichte eventuell weitere Parameter angeben.

Sie können auch Parameter angeben, um den Inhalt des Berichts zu filtern. Damit können Sie unter Angabe von Benutzerkontenattributen, geografischem Standort, Netzwerkstruktur, Organisationseinheit oder Geschäftsbereich den Bericht auf bestimmte Datensätze beschränken. Mit zusätzlichen Parametern können Sie in einigen Berichten die Reihung der Datensätze kontrollieren oder statistische Schwellenwerte für Diagramme und Grafiken festlegen.

Die folgenden Parameter werden zur Erstellung von Berichten verwendet. Für einige Berichte stehen nicht alle Parameter zur Verfügung.

Konfiguration

Gibt die Konfiguration an, auf der der Bericht basiert. Die Dropdown-Listen zeigen alle Konfigurationsdateien der CA RCM-Datenbank an.

Verwenden Sie die folgenden Parameter, um Berichte zu erstellen, die sich auf Benutzer-, Rollen- oder Ressourcenattribute beziehen:

Nach Feld

Legt in der Konfigurationsdatei ein Datenfeld fest, das zum Filtern und Sortieren von Datensätzen verwendet wird. Die Dropdown-Liste zeigt bestehende Datenfelder in der durch den Parameter **Konfiguration** festgelegten Konfigurationsdatei an. Nur relevante Datenfelder werden angezeigt - zum Beispiel werden für Berichte, die nach Benutzerkonto angeordnet wurden, nur Benutzerattribute angezeigt.

Von/Bis

Legt auf der Basis des im Parameter **Nach Feld** festgelegten Datenfeldes den Bereich der Datensätze fest, die der Bericht enthalten soll. Die Dropdown-Listen zeigen bereits vorhandene Feldwerte, die von der angegebenen Konfigurationsdatei abgerufen wurden.

Muster

Legt eine mit einem Muster übereinstimmende Zeichenfolge fest, die in den Bericht aufzunehmende Datensätze aus der angegebenen Konfigurationsdatei auswählt. Die Zeichenfolge wird als Filter auf das im Parameter **Nach Feld** festgelegte Datenfeld angewendet. Das Muster muss der Verwendung folgen, die für die Musterklasse 'java.utils.regex.Pattern' in der von dieser Ausgabe unterstützten Java-Version festgelegt ist.

Verwenden Sie die folgenden Parameter, wenn Sie mit Analyse-/Statistikberichte arbeiten, die sich auf die Auditkarte der ausgewählten Konfiguration beziehen:

Auditkarte

Legt die Auditkarte fest, von der analytische Informationen abgerufen werden, um den Bericht zu erstellen. Die Dropdown-Liste zeigt alle Auditkarten, die der angegebenen Konfigurationsdatei zugeordnet sind.

Mindestbewertung

Legt einen Schwellenwert für die in den Bericht aufzunehmenden Informationen fest. Dieser Filter wird auf die vom Parameter **Auditkarte** festgelegte Auditkarte angewendet. Auditkriterien, deren Bewertung unter dem Schwellenwert liegt, werden nicht in den Bericht aufgenommen. Verwenden Sie diesen Filter, um auditierte Bedingungen auszuschließen, die in der festgelegten Konfiguration nicht vorherrschend oder nicht wichtig sind.

Von Warnungs-ID/Zu Warnungs-ID

Legt einen Bereich für in den Bericht aufzunehmende Warnungs-IDs fest. Die Dropdown-Liste zeigt vorhandene Warnungs-ID-Werte auf der vom Parameter **Auditkarte** festgelegten Auditkarte.

Warnungstyp:

Gibt eine analytische Warnung an, die als Filter verwendet wird. Nur Warnungen des angegebenen Typs sind im Bericht enthalten. Die Dropdown-Liste zeigt alle standardmäßigen analytischen Warnungen, die sich auf der vom Parameter **Auditkarte** spezifizierten Auditkarte befinden.

Von (Datum)/Bis (Datum)

Geben Sie einen zeitbezogenen Filter für Auditkartendaten an. Der Bericht schließt nur analytische Warnungen ein, die im angegebenen Zeitrahmen aufgezeichnet wurden. Dieser Filter wird auf die vom Parameter **Auditkarte** festgelegte Auditkarte angewendet.

Verwenden Sie die folgenden Parameter für Berichte über die Richtlinienüberprüfung von Geschäftsregeln:

Richtlinien

Legt eine Datei für Geschäftsprozessregeln (BPR) fest, die dazu verwendet wird, Berichtsdaten zu filtern. Nur Warnungen, die mit den festgelegten BPR im Zusammenhang stehen, sind im Bericht enthalten. Die Dropdown-Liste zeigt alle BPR-Dateien der CA RCM-Datenbank an.

Verwenden Sie die folgenden Parameter für Berichte zum Vergleich der Methodologien für die Rollenmodellierung:

Masterkonfiguration

Legt die Konfiguration fest, die beim Vergleichen von mehreren Konfigurationen als Referenz verwendet wird. Die Dropdown-Liste zeigt alle Konfigurations-Dateien der Datenbank an.

Beschriftung der Masterkonfiguration

Definiert eine einen Text enthaltende Bezeichnung für die Konfiguration der Referenz.

Konfiguration *n*

Legt eine Konfiguration fest, die mit der Masterkonfiguration verglichen wird. Die Dropdown-Liste zeigt alle Konfigurations-Dateien der Datenbank an.

Bezeichnung

Definiert eine einen Text enthaltende Bezeichnung für die entsprechende Konfiguration.

Verwenden Sie die folgenden Parameter, wenn Sie mit Berichten über Kampagnen arbeiten:

Kampagne

Legt die Kampagne fest, die der Bericht als Referenz verwenden wird. Die Dropdown-Liste zeigt alle im Portal definierten Kampagnen.

Alle Genehmiger

Alle Teilnehmer, die Berechtigungen für von ihnen verwaltete Benutzer oder Ressourcen genehmigen müssen, sind in dem Bericht enthalten.

Nach Feld auswählen

Legt ein Benutzerattributfeld fest, das zur Auswahl von Teilnehmern verwendet wird. Die Dropdown-Liste enthält alle Benutzerattribute, die in der mit der Kampagne verbundenen Konfigurationsdatei festgelegt sind. Wählen Sie ein Attribut, woraufhin bestehende Werte in der Konfigurationsdatei aufgelistet werden. Klicken Sie auf einen Wert, um ihn als Filter zu verwenden. Nur Teilnehmer mit diesem Attributwert sind im Bericht enthalten.

Verwenden Sie die folgenden Parameter bei Lebenszyklusberichten:

Universum

Legt das Universum fest, das der Bericht als Referenz verwenden wird. Die Dropdown-Liste zeigt alle im Portal definierten Universen.

Konfigurationen

Legt die für den Bericht zu verwendenen Konfigurationen im Universum fest.

Entitätstyp

Legt die Entität fest, die der Bericht umfassen wird.

Nach Feld

Legt ein Datenfeld fest, das zum Filtern von Teilnehmern verwendet wird. Die Dropdown-Liste zeigt alle Datenfelder an, die für den ausgewählten Entitätstyp in den angegebenen Konfigurationsdateien festgelegt sind. Wählen Sie ein Attribut aus, woraufhin bestehende Werte aufgelistet werden. Klicken Sie auf einen Wert, um ihn als Filter zu verwenden.

Von (Datum)

Gibt das Startdatum des Berichts an. Änderungen an ausgewählten Entitäten seit dem Anfangsdatum werden in den Bericht eingeschlossen.

Aktuelle Links anzeigen

Nimmt zu anderen Entitäten bestehende Links in den Bericht auf.

Einen Berichtsindex anzeigen

Manche Berichte werden von dem zum Filtern und Sortieren des Berichts verwendeten Datenfeld mit einem Index versehen. Sie können diesen Index dazu verwenden, auf Ihrem Browser in dem Bericht zu navigieren.

Um einen Berichtsindex anzuzeigen, klicken Sie hier . Auf der linken Seite des Fensters öffnet sich ein Navigationsbereich.

Verändern Sie Berichtparameter

Sie können den Bericht mit anderen Parametereinstellungen neu erstellen. Dies ist hilfreich, wenn der Umfang des Berichts nicht Ihren Vorstellungen entspricht, oder wenn Sie parallele Informationsteile vergleichen möchten - zum Beispiel unterschiedliche Standorte oder Geschäftsbereiche.

So erstellen Sie den Bericht neu:

1. Klicken Sie auf den Link "Parameter anzeigen" auf der linken Seite der Berichtsanzeige.

   Der Parameterdialog für diesen Bericht öffnet sich und die derzeitigen Einstellungen werden angezeigt.

2. Verändern Sie die Parametereinstellungen nach Ihren Vorstellungen und klicken Sie auf "OK".

   Der gleiche Bericht wird unter Anwendung der neuen Einstellungen erstellt.

   Hinweis: Die vorherige Version des Berichts wurde überschrieben. Um die ältere Version zu bewahren, drucken Sie sie aus oder exportieren Sie sie, bevor Sie den Bericht mit neuen Parametern erstellen.

Exportieren Sie einen Bericht zu einer Datei.

Sie können Berichte in verschiedenen geläufigen Formaten speichern. Sie können sie so mit anderen teilen und sie anderen Dokumenten beifügen.

So exportieren Sie einen Bericht zu einer Datei

1. Klicken Sie auf die linke Seite des Fensters.

   Das Dialogfeld "Exportbericht" wird angezeigt.

2. So wählen Sie das Dokumentformat, den Ausgabebereich und die Größenbestimmungsoptionen aus. Klicken Sie auf "**OK"**.

   Beim Erstellen des Dokuments wird eine Aufforderung angezeigt.

3. Führen Sie einen der folgenden Schritte aus:

   - Klicken Sie zum Speichern der Datei auf **"Speichern"**.
   - Wählen Sie **Öffnen** aus, um die Datei anzuzeigen.

Drucken Sie einen Bericht

Sie können Berichte an einen Drucker senden, um Informationen zu teilen oder zu archivieren, oder um die Überprüfung großformatiger Berichte zu vereinfachen.

So drucken Sie einen Bericht

1. Klicken Sie auf die linke Seite des Berichtfensters.

   Das Dialogfeld "Druckerbericht" wird angezeigt.

2. Wählen Sie ein Ausgabeformat und einen Druckbereich aus, und klicken Sie auf "OK".

   Eine Druckvorschau wird in einem neuen Browser-Fenster angezeigt.

3. So konfigurieren Sie Druckereinstellungen und drucken Sie.

Kapitel 11: Bearbeiten von Geschäftsprozessregeln

Dieses Kapitel enthält folgende Themen:

Konzepte der Geschäftsprozessregeln

Eine Geschäftsprozessregel (BPR) drückt Beschränkungen im Bereich Unternehmen, Bereitstellung oder Sicherheit als logische Bedingung aus, die auf die Entitäten oder Links in der CA RCM-Konfiguration angewendet werden können. Beispiel:

`<Einkauf>` **`darf nicht übereinstimmen mit`** `<Zahlung an Zulieferer>`

Sie können diese Anweisung auf eine CA RCM-Konfiguration anwenden, um sicherzustellen, dass Mitarbeiter, die Bestellungen an Zulieferern ausgeben können, über keine Rollen verfügen, die Zahlungsberechtigungen gewähren, um jene Zulieferer zu bezahlen.

Normalerweise wird eine BPR durch das Angeben der folgenden Information angegeben:

- Die Art der Regel – CA RCM bietet eine große Auswahl an Regeln, mit denen Sie verschiedene Entitätswerte überprüfen und vergleichen können. Der Rollentyp im oben genannten Beispiel ist zum Beispiel "Zugriff von Benutzern auf Rollen nach Rollenzugriff beschränken". Dieser Regeltyp beschränkt die Rollen, die ein Benutzer haben kann, basierend auf den bereits vorhandenen Rollen des Benutzers.
- Logische Bedingung – In unserem Beispiel ist es Benutzern mit gewissen Rollen verboten, bestimmte Rollen zu haben. Sie können diesen Regeltyp auch verwenden, um Benutzern mit gewissen Rollen zu erlauben bzw. von ihnen zu verlangen, andere Rollen zu haben.
- Datensätze und Grenzwerte – In unserem Beispiel definieren wir einerseits Rollen, die im Zusammenhang mit Einkaufsfunktionen stehen, und andererseits Rollen, die berechtigt sind, Zahlungen zu bewilligen.

Eine Geschäftsrichtlinie besteht aus mehreren BPRs. Diese Richtlinie (als ".bpr" gespeichert) ist unabhängig bestimmter Konfigurationen vorhanden. Die Regeln, die die Richtlinie umfasst, können angepasst und auf CA RCM-Konfigurationen angewandt werden, um Logik, Integrität und Compliance mit der Richtlinie zu überprüfen.

Weitere Informationen:

Arten der Geschäftsprozessregel (siehe Seite 185)

Arten der Geschäftsprozessregel

Die meisten Regeln beschreiben eine Beziehung zwischen zwei Gruppen von Entitäten. Sie geben die Mitglieder dieser Gruppen an, wenn Sie eine Regel erstellen oder bearbeiten. Diese Gruppen werden im Fenster zur Bearbeitung der BPR als "A" und "B" oder "Links" und "Rechts" dargestellt. In der folgenden Tabelle werden die verschiedenen verfügbaren Regeltypen sowie der logische Operator beschrieben, den die einzelnen Regeln verwenden.

Rolle - Rolle (nach Benutzern)

Wenn eine Konfiguration Rollen A und B enthält, gilt das Folgende:

Nur <L> darf <R> beinhalten

Nur Benutzer, die Rollen unter A haben (links), dürfen Rollen unter B haben (rechts).

<L> muss <R> beinhalten

Benutzer, die Rollen unter A haben (links), müssen Rollen unter B haben (rechts).

<L> darf nicht <R> beinhalten

Benutzer, die Rollen unter A haben (links), dürfen keine Rollen unter B haben (rechts).

<L> darf nur <R> beinhalten

Benutzer, die Rollen in A haben (links), können nur Rollen in B (rechts) haben, jedoch keine anderen

Rolle - Rolle (nach Rollen)

Wenn eine Konfiguration Rollen A und B enthält, gilt das Folgende:

Nur <L> darf <R> beinhalten

Nur Rollen, die untergeordnete Rollen in A haben (links), dürfen Rollen in B (rechts) als untergeordnete Objekte haben

<L> muss <R> beinhalten

Rollen, die untergeordnete Rollen in A haben (links), müssen Rollen in B (rechts) als untergeordnete Objekte haben

<L> darf nicht <R> beinhalten

Rollen, die untergeordnete Rollen in A haben (links), dürfen keine Rollen in B (rechts) als untergeordnete Objekte haben

<L> darf nur <R> beinhalten

Rollen, die untergeordnete Rollen in A haben (links), können nur Rollen in B (rechts) als untergeordnete Objekte haben, jedoch keine anderen

Rolle - Ressource (nach Benutzern)

Wenn eine Konfiguration Rollen A und Ressourcen B enthält, gilt das Folgende:

Nur <L> darf <R> beinhalten

Nur Benutzer, die Rollen unter A haben (links), dürfen Zugriff auf Ressourcen unter B haben (rechts)

<L> muss <R> beinhalten

Benutzer, die Rollen unter A haben (links), müssen auf Ressourcen unter B zugreifen (rechts)

<L> darf nicht <R> beinhalten

Benutzer, die Rollen unter A haben (links), dürfen nicht auf Ressourcen unter B zugreifen (rechts)

<L> darf nur <R> beinhalten

Benutzer, die Rollen in A haben (links), können nur auf Ressourcen in B (rechts) haben, jedoch auf keine anderen

Rolle - Ressource (nach Rollen)

Wenn eine Konfiguration Rollen A und Ressourcen B enthält, gilt das Folgende:

Nur <L> darf <R> beinhalten

Nur übergeordnete Rollen der Rollen in A (links) können auf Ressourcen in B zugreifen (rechts)

<L> muss <R> beinhalten

Übergeordnete Rollen der Rollen in A (links) müssen auf Ressourcen in B zugreifen (rechts)

<L> darf nicht <R> beinhalten

Übergeordnete Rollen der Rollen in A (links) dürfen nicht auf Ressourcen in B zugreifen (rechts)

<L> darf nur <R> beinhalten

Übergeordnete Rollen der Rollen in A (links) können nur auf Ressourcen in B (rechts) zugreifen, jedoch auf keine anderen

Ressource - Ressource (nach Benutzern)

Wenn eine Konfiguration Ressource A und B enthält, gilt das Folgende:

Nur <L> darf <R> beinhalten

Nur Benutzer, die Zugriff auf Ressourcen unter A haben (links), dürfen Zugriff auf Ressourcen unter B haben (rechts)

<L> muss <R> beinhalten

Benutzer, die Zugriff auf Ressourcen unter A haben (links), müssen Zugriff auf Ressourcen unter B haben (rechts)

<L> darf nicht <R> beinhalten

Benutzer, die Zugriff auf Ressourcen unter A haben (links), dürfen keinen Zugriff auf Ressourcen unter B haben (rechts)

<L> darf nur <R> beinhalten

Benutzer, die Zugriff auf Ressourcen in A haben (links), haben nur Zugriff auf Ressourcen in B (rechts), jedoch auf keine anderen

Ressource – Ressource (nach Rollen)

Wenn eine Konfiguration Ressource A und B enthält, gilt das Folgende:

Nur <L> darf <R> beinhalten

Nur Rollen, die Ressourcen in A einschließen (links), können Ressourcen in B einschließen (rechts)

<L> muss <R> beinhalten

Rollen, die Ressourcen in A einschließen (links), müssen Ressourcen in B einschließen (rechts)

<L> darf nicht <R> beinhalten

Rollen, die Ressourcen in A einschließen (links), dürfen keine Ressourcen in B einschließen (rechts)

<L> darf nur <R> beinhalten

Rollen, die Ressourcen in A einschließen (links), können nur Ressourcen in B einschließen (rechts), jedoch keine anderen

Benutzerattribut – Rolle

Wenn eine Konfiguration den Benutzerattributsatz A und Rollensatz B enthält, gilt das Folgende:

Nur <L> darf <R> beinhalten

Nur Benutzer, die Benutzerattribute unter A haben (links), dürfen Rollen unter B haben (rechts)

<L> muss <R> beinhalten

Benutzer, die Benutzerattribute unter A haben (links), müssen Rollen unter B haben (rechts)

<L> darf nicht <R> beinhalten

Benutzer, die Benutzerattribute unter A haben (links), dürfen keine Rollen unter B haben (rechts)

<L> darf nur <R> beinhalten

Benutzer, die Benutzerattribute in A haben (links), können nur Rollen in B haben (rechts), jedoch keine anderen

Benutzerattribut - Rollenattribut

Wenn eine Konfiguration den Benutzerattributsatz A und Rollenattributsatz B enthält, gilt das Folgende:

Nur <L> darf <R> beinhalten

Nur Benutzer, die Attribute unter A haben (links), dürfen Rollen mit Attributen unter B haben (rechts)

<L> muss <R> beinhalten

Benutzer, die Attribute unter A haben (links), müssen Rollen mit Attributen unter B haben (rechts)

<L> darf nicht <R> beinhalten

Benutzer, die Attribute unter A haben (links), dürfen keine Rollen mit Attributen unter B haben (rechts)

<L> darf nur <R> beinhalten

Benutzer, die Attribute in A haben (links), können nur Rollen mit Attributen in B haben (rechts), jedoch keine anderen

Benutzerattribute – Ressource

Wenn eine Konfiguration den Benutzerattributsatz A und Ressourcensatz B enthält, gilt das Folgende:

Nur <L> darf <R> beinhalten

Nur Benutzer, die Benutzerattribute unter A haben (links), dürfen Zugriff auf Ressourcen unter B haben (rechts)

<L> muss <R> beinhalten

Benutzer, die Benutzerattribute unter A haben (links), müssen Zugriff auf Ressourcen unter B haben (rechts)

<L> darf nicht <R> beinhalten

Benutzer, die Benutzerattribute unter A haben (links), dürfen keinen Zugriff auf Ressourcen unter B haben (rechts)

<L> darf nur <R> beinhalten

Benutzer, die Attribute in A haben (links), können nur Zugriff auf Ressourcen in B haben (rechts), jedoch auf keine anderen

Benutzerattribut - Benutzerattribut

Wenn eine Konfiguration Benutzerattribute A und B enthält, gilt das Folgende:

Nur <L> darf <R> beinhalten

Nur Benutzer, die Benutzerattribute unter A haben (links), dürfen Attribute unter B haben (rechts)

<L> muss <R> beinhalten

Benutzer, die Benutzerattribute unter A haben (links), müssen Attribute unter B haben (rechts)

<L> darf nicht <R> beinhalten

Benutzer, die Benutzerattribute unter A haben (links), dürfen keine Attribute unter B haben (rechts)

<L> darf nur <R> beinhalten

Benutzer, die Attribute in A haben (links), können nur Attribute in B haben (rechts), jedoch keine anderen

Trennung von Pflichtrollen

Für einen Satz von Rollen L und einen numerischen Wert R:

Sollte nicht mehr als <R> von <L> haben

Benutzer sollten nicht mehr als R der Rollen unter haben.

Sollte mindestens <R> von <L> haben

Benutzer sollten mindestens R der Rollen unter L haben.

Sollte genau <R> von <L> haben

Benutzer müssen genau R der Rollen in L haben.

Trennung von Pflichtressourcen

Für einen Satz von Ressourcen L und einen numerischen Wert R:

Sollte nicht mehr als <R> von <L> haben

Benutzer sollten nicht mehr als R der Ressourcen unter L haben.

Sollte mindestens <R> von <L> haben

Benutzer sollten mindestens R der Ressourcen unter L haben.

Sollte genau <R> von <L> haben

Benutzer müssen genau R der Ressourcen in L haben.

Benutzer-Zähler von Rollen

Für einen Satz von Rollen L und einen numerischen Wert R:

Sollte nicht mehr als <R> Benutzer haben

Rollen in L sollten nicht mehr als R Benutzer haben.

Sollte mindestens <R>Benutzer haben

Rollen in L sollten mindestens R Benutzer haben.

Sollte genau <R> Benutzer haben

Rollen in L müssen genau R Benutzer haben.

Benutzer-Zähler von Ressourcen

Für einen Satz von Ressourcen L und einen numerischen Wert R:

Sollte nicht mehr als <R> Benutzer haben

Ressourcen in L sollten nicht mehr als R Benutzer haben.

Sollte mindestens <R>Benutzer haben

Ressourcen in L sollten mindestens R Benutzer haben.

Sollte genau <R> Benutzer haben

Ressourcen in L müssen genau R Benutzer haben.

Wert des Benutzerattributs

Zahl <L> muss größer sein als <R>

Der numerische Wert des Benutzerattributs für die linke Entität muss größer sein als der numerische Wert der rechten Entität.

Zahl <L> muss kleiner sein als <R>

Der numerische Wert des Benutzerattributs für die linke Entität muss kleiner sein als der numerische Wert der rechten Entität.

Zahl <L> muss <R> entsprechen

Der numerische Wert des Benutzerattributs für die linke Entität muss dem numerischen Wert der rechten Entität entsprechen.

Datum <L> muss vor <R> liegen

Das Datum für die Benutzerattribute der linken Entität muss vor dem Datum der rechten Entität liegen.

Datum <L> muss nach <R> liegen

Das Datum für die Benutzerattribute der linken Entität muss nach dem Datum der rechten Entität liegen.

<L> muss regulärem Ausdruck <R> entsprechen

Der Wert für die Benutzerattribute der linken Entität muss dem Wert des regulären Ausdrucks unter der rechten Entität entsprechen.

<L> darf nicht regulärem Ausdruck <R> entsprechen

Der Wert für die Benutzerattribute der linken Entität dürfen nicht dem Wert des regulären Ausdrucks unter der rechten Entität entsprechen.

<L> sollte leer sein

Der Wert für das unter der linken Entität ausgewählte Benutzerattribut sollte leer sein.

<L> sollten nicht leer sein

Der Wert für das unter der linken Entität ausgewählte Benutzerattribut sollte nicht leer sein.

Erstellen und Bearbeiten von Geschäftsprozessregeln im CA RCM-Portal

Der BPR-Assistent vereinfacht die Erstellung von Geschäftsprozessregeln.

Hinweis: Wenn Sie eine vorhandene Regel bearbeiten, enthält das Fenster "BPR bearbeiten" nur die Optionen des Assistenten, die relevant für den Regeltyp sind, den Sie bearbeiten.

Arbeiten Sie sich wie folgt durch die Fenster des Assistenten:

1. Geben Sie im Fenster "Grundlegende Informationen" Informationen an, die den Umfang und Zweck der Regel beschreiben. Folgende Felder sind nicht selbsterklärend:

   Bewertung

   Ein numerischer Wert, der die Bedeutung einer Verletzung dieser Regel beschreibt, im Vergleich zu Verletzungen anderer Regeln in der Richtlinie.

   Eigentümer

   Definiert den für die Regel verantwortlichen Benutzer.

   Geschäftsbereich/Geschäftsprozess

   Textfelder, die den Umfang und Zweck der Regel angeben. Diese Felder dienen nur der Beschreibung und wirken sich nicht auf die Verarbeitung der Regel aus.

2. Geben Sie im Fenster "Logik" Werte für die folgenden Felder an, um die zu Grunde liegende Logik der Regel zu bestimmen:

   Typ

   Gibt den Typ der Entitäten, Links oder Attribute an, die geprüft werden, um Verletzungen zu identifizieren.

   Einschränkung

   Gibt die angewandte Einschränkung geprüfter Entitäten an.

3. Im Fenster "Daten" geben Sie die Entitäten an, die geprüft werden. Sie können einzelne Entitäten auswählen, oder Attributwerte angeben, um eine Gruppe von Entitäten auszuwählen.

   Viele Regeltypen vergleichen zwei Entitätssätze. In diesen Fällen wird das Fenster "Daten" in zwei Bereiche, links und rechts, geteilt, und die Logik der Regel wird in Bezug auf diese beiden Gruppen angegeben.

   Für andere Regeltypen geben Sie numerische Grenzwerte, Datumsbereiche oder Textabstimmungsmuster an.

4. Das Fenster "Zusammenfassung" zeigt die Regeleinstellungen und lässt Sie die Regel auf die Referenzkonfiguration testen, bevor Sie die Regel erstellen.

Arbeiten mit Geschäftsrichtlinien im CA RCM-Portal

Befolgen Sie diese allgemeinen Prozeduren, wenn Sie mit BPR-Dateien im CA RCM-Portal arbeiten.

Hinweis: Sie können die BPR-Dateien auch im DNA-Client-Tool bearbeiten. Es gibt einige Unterschiede zwischen den beiden Oberflächen. So können Sie zum Beispiel in der DNA-Oberfläche Entitätsgruppen angeben, indem Sie sie aus einer offenen Konfigurationsdatei auswählen. Im Portal vereinfacht ein Assistent die Dateibearbeitung. Sie können auch das Client-Tool zur Datenverwaltung verwenden, um BPR-Dateien in die Datenbank zu importieren. Weitere Informationen zur Bearbeitung von BPR in DNA finden Sie im *DNA-Benutzerhandbuch* und im *Benutzerhandbuch zur Datenverwaltung*.

Um auf BPR-Tools zuzugreifen, klicken Sie im Portal auf "Verwaltung" und anschließend auf "BPR-Management". Das Fenster "BPR-Liste" wird angezeigt. Die Tabelle listet alle Dateien der Geschäftsrichtlinien in der Datenbank auf.

Über dieses Fenster können Sie folgende Aktionen durchführen:

- Um eine Datei der Geschäftsrichtlinie zu erstellen, klicken Sie auf "Erstellen".
- Um eine vorhandene Datei der Geschäftsrichtlinie zu bearbeiten, klicken Sie neben der entsprechenden Datei auf "Bearbeiten".
- Um eine vorhandene Datei der Geschäftsrichtlinie auf einer Konfiguration auszuführen, klicken Sie auf "Ausführen".
- Um eine Datei der Geschäftsrichtlinie aus der Datenbank zu entfernen, klicken Sie neben der entsprechenden Datei auf "Löschen".

Erstellen von Dateien der Geschäftsrichtlinie im CA RCM-Portal

Erstellen Sie eine Datei der Geschäftsrichtlinie, um eine Reihe von BPRs auf eine CA RCM-Konfiguration anzuwenden.

So erstellen Sie Dateien der Geschäftsrichtlinie im CA RCM-Portal

1. Gehen Sie im CA RCM-Portal auf "Verwaltung" und danach auf "BPR-Management".

   Das Fenster "BPR-Liste" wird angezeigt. Die Tabelle listet alle Dateien der Geschäftsrichtlinien in der Datenbank auf.

2. Klicken Sie auf "Neue hinzufügen".

   Das Fenster "BPRs erstellen" wird angezeigt.

3. Geben Sie Einstellungen für die Richtlinie an. Das folgende Feld ist nicht selbsterklärend:

   Referenzkonfiguration

   Die Konfiguration, die zum Erstellen und Testen der Richtliniendatei verwendet wird.

   Hinweis: Die Dateien der Geschäftsrichtlinie sind unabhängig von den Konfigurationsdateien. Die Referenzkonfiguration wird ausschließlich zum Erstellen und Testen der Richtlinie verwendet. Sie können die abgeschlossene Geschäftsrichtlinie auf beliebige Konfigurationen anwenden.

4. Geben Sie optionale Verhalten für die Richtliniendatei unter Richtlinienattributen an. Es stehen unter anderem folgende Optionen zur Verfügung:

   Schreibgeschützt

   Gibt an, ob Sie die Datei bearbeiten können.

   Protokolliert

   Gibt an, ob Änderungen der Datei im Transaktionsprotokoll aufgezeichnet werden.

   Abgeschlossen

   Dieses Feld ist derzeit ohne Verwendung.

5. Klicken Sie auf "Speichern".

   Die Datei der Geschäftsrichtlinie wird in der Datenbank erstellt.

   Das Fenster "BPRs bearbeiten" wird angezeigt.

6. Verwenden Sie die Bearbeitungs-Tools dieses Fensters (siehe Seite 196), um Regeln in der Richtlinie zu definieren und zu ändern.

Weitere Informationen:

Erstellen einer Datei der Geschäftsrichtlinie im CA RCM-Portal (siehe Seite 196)

Ausführen von Geschäftsrichtlinienregeln im CA RCM-Portal

Wenn Sie eine Datei der Geschäftsrichtlinie auf eine Konfiguration anwenden, analysiert CA RCM die Konfiguration, um Entitäten und Links zu finden, die die Regeln der Richtlinie verletzen. Das Ergebnis ist eine Auditkarte, die alle Verletzungen der Richtlinie enthält, die in der Konfiguration festgestellt wurde.

So führen Sie Regeln der Geschäftsrichtlinie im CA RCM-Portal aus

1. Klicken Sie im Hauptmenü des Portals auf "Verwaltung" und anschließend auf "BPR-Management".

   Das Fenster "BPR-Liste" wird angezeigt. Die Tabelle listet alle Regeln der Geschäftsrichtlinien in der Datenbank auf.

2. Klicken Sie auf "Ausführen".

   Das Fenster "BPRs ausführen" wird angezeigt.

3. Geben Sie Werte für folgende Felder an:

   Auditkarte

   Definiert den Namen der Auditkarte, die in der Zielkonfiguration festgestellte Verletzungen enthält.

   Konfiguration

   Gibt eine Konfigurationsdatei in der Datenbank an, die das Ziel für Analysen von Geschäftsrichtlinien ist.

4. Wählen Sie im Bereich "BPRs auswählen" die Dateien der Geschäftsrichtlinie aus, die Sie auf die Zielkonfiguration anwenden wollen.
5. Klicken Sie auf "Ausführen".

   Die Auditkarte wird erstellt, und die Analyse der Konfigurationsdatei beginnt. Wenn keine Verletzungen festgestellt werden, wird die leere Auditkarte aus der Datenbank gelöscht.

Erstellen einer Datei der Geschäftsrichtlinie im CA RCM-Portal

Sie können unterschiedliche Einstellungen für Dateien der Geschäftsrichtlinie verändern, oder die Richtlinienregeln in der Datei bearbeiten.

So erstellen Sie eine Datei der Geschäftsrichtlinie im CA RCM-Portal

1. Klicken Sie im Hauptmenü des Portals auf "Verwaltung" und anschließend auf "BPR-Management".

   Das Fenster "BPR-Liste" wird angezeigt. Die Tabelle listet alle Dateien der Geschäftsrichtlinien in der Datenbank auf.

2. Klicken Sie neben der Datei, die Sie ändern möchten, auf "Bearbeiten".

   Das Fenster "BPRs bearbeiten" wird angezeigt.

3. Ändern Sie die Einstellungen für die Richtliniendatei. Folgende Felder sind nicht selbsterklärend:

   Referenzkonfiguration

   Die Konfiguration, die zum Erstellen und Testen der Richtliniendatei verwendet wird.

   Hinweis: Die Dateien der Geschäftsrichtlinie sind unabhängig von den Konfigurationsdateien. Die Referenzkonfiguration wird ausschließlich zum Erstellen und Testen der Richtliniendatei verwendet. Sie können die abgeschlossene Geschäftsrichtlinie auf beliebige Konfigurationen anwenden.

4. Geben Sie optionale Verhalten für die Richtliniendatei im Bereich "Richtlinienattribute" des Fensters an. Vorhandene Optionen:

   Schreibgeschützt

   Gibt an, ob andere die Datei bearbeiten können.

   Protokolliert

   Gibt an, ob Änderungen der Datei im Transaktionsprotokoll aufgezeichnet werden.

   Abgeschlossen

   Dieses Feld ist derzeit ohne Verwendung.

5. Die Tabelle im Zentrum des Fensters listet die Regeln der Richtlinie auf. Um die Regeln zu ändern, führen Sie eine dieser Aktionen aus:

   - Klicken Sie auf "Regel hinzufügen", um eine Regel zu erstellen (siehe Seite 192).
   - Klicken Sie neben einer Regel auf "Bearbeiten", um eine vorhandene Regel zu ändern (siehe Seite 192).
   - Klicken Sie neben einer Regel auf "Löschen", um sie aus der Richtliniendatei zu löschen.
   - Klicken Sie auf "Test", um den Regelsatz auf die Referenzkonfiguration zu testen.

6. Klicken Sie auf "Speichern".

   Änderungen der Richtliniendatei werden in der Datenbank gespeichert.

Kapitel 12: Verwenden von Verwaltungsfunktionen

Das Verwaltungsmenü bietet einige wichtige Vorgänge, die nur von Administratoren mit den entsprechenden Berechtigungen ausgeführt werden können.

Dieses Kapitel enthält folgende Themen:

Verwendung des Ticket-Managementsystems

CA RCM implementiert Datenconnectorjobs und andere administrative Aufgaben mittels eines ticketbasierten Prozess-Management-Systems. Sie verwalten diese Ticketwarteschlangen in anderen Fenstern als den für Geschäfts-Workflows verwendeten Fenstern.

Ansichten des Posteingangs

Greifen Sie auf die folgenden vordefinierten Ticketwarteschlangenfenster unter "Posteingang" im CA RCM-Hauptmenü zu:

Geöffnet/Neu/Abgeschlossen

Zeigt Tickets mit dem Status "Offen", "Neu" oder "Fertig".

Neue Tickets

Zeigt neue Tickets.

Überfällige Tickets

Zeigt Tickets, deren Enddatum bereits in der Vergangenheit liegt.

Genehmigertickets

Zeigt die Genehmigertickets des aktuellen Benutzers.

Hinweis: Dieses Fenster ist immer leer. Verwendung der Fenster "Meine Aufgaben", "Meine Anfragen" oder "Workflows", um mit Genehmigungsaktionen für Geschäfts-Workflows zu arbeiten.

Kampagnentickets

Zeigt Kampagnentickets.

Hinweis: Dieses Fenster ist immer leer. Verwendung der Fenster "Meine Aufgaben", "Meine Anfragen" oder "Workflows", um mit Aufgaben und Aktionen von Zertifizierungskampagnen zu arbeiten.

Archivierte Tickets

Zeigt Tickets, die archiviert wurden.

Tickets gruppieren sich in Baumstrukturen, basierend auf den administrativen Vorgängen, auf die sie bezogen sind.

Weitere Informationen:

Felder in Workflow-Fenstern (siehe Seite 69)

Admin-Ansicht / Benutzeransicht

Die Schaltfläche "Admin-Ansicht/Benutzeransicht" ermöglicht es Ihnen, zwischen den beiden Ansichten der Ticketwarteschlange zu wechseln:

Benutzeransicht

Die Warteschlange zeigt nur Tickets für Prozesse an, die der Benutzer initiiert hat.

Admin-Ansicht

Die Warteschlange zeigt alle Tickets im System an, sogar jene, die von anderen Managern erstellt wurden.

Die Admin-Ansicht steht nur einem übergeordneten Administrator zur Verfügung. Die Schaltflächen sind nur für jene Benutzer sichtbar, die mit der in "eurekify.properties" als Systemadministratorrolle definierten Rolle verknüpft sind. Die Standardoption lautet wie folgt:

```
sage.admin.role=CA RCM-Admin-Rolle
```

Weitere Informationen:

Sicherheit und Berechtigungen (siehe Seite 285)
CA RCM-Eigenschaften (siehe Seite 311)

Formular für Ticketeigenschaften

Wenn Sie ein Ticket anklicken, zeigt ein Dialogfenster detaillierte Informationen für dieses Ticket an. Der Inhalt dieses Fensters hängt vom Typ des Tickets ab, das angezeigt wird.

Der obere Teil des Fensters wird nie abgeändert und enthält die Ticketinformationen:

Feld	Beschreibung
<Tickettitel>	Der angezeigte Tickettyp ist in der ersten Zeile des Fensters zu finden.
Ticket-ID	Jedes Ticket hat eine eindeutige Ticket-ID.
Eigentümer	Der Eigentümer des bestimmten Tickets. Die Funktionen des Tickets hängen davon ab, wer das Ticket gerade einsieht. Nur der Eigentümer hat vollständigen Zugriff auf alle für einen bestimmten Tickettyp vorhandenen Funktionen.

Feld	Beschreibung
Vorheriger Eigentümer	In Kampagnen oder Genehmigungsvorgängen können Tickets an andere Manager delegiert oder eskaliert werden. Wenn ein Ticket von einem anderen Benutzer an den Eigentümer gesendet wird, wird dieser Benutzername (nicht der aktuelle Eigentümer) in diesem Feld angezeigt.
Status	Gibt den Ticketstatus an.
Fälligkeitsdatum	Jedes Ticket hat ein Fälligkeitsdatum. Bis zu diesem Zeitpunkt müssen die Aktionen des Tickets ausgeführt werden.
Priorität	Gibt den aktuellen Prioritätsstand an. Es sind folgende Optionen verfügbar: ■ Niedrig ■ Normal ■ Dringend ■ Kritisch
Schweregrad	Gibt den aktuellen Schweregrad an. Es sind folgende Optionen verfügbar: ■ Minimal ■ Mittel ■ Schwerwiegend ■ Dringend ■ Kritisch
Status	Gibt den aktuellen Zustand des Tickets an. Es sind die folgenden Optionen verfügbar: ■ Neu ■ Offen ■ Ausgeblendet ■ Fertig ■ Archiviert ■ Abgebrochen
Änderungsdatum	Gibt den Zeitpunkt an (Datum und Uhrzeit), an dem das Ticket zum letzten Mal geändert wurde.
Erstellungsdatum	Gibt den Zeitpunkt an (Datum und Uhrzeit), an dem das Ticket erstellt wurde.
Titel	Der Titel des Tickets.
Beschreibung	Eine Beschreibung des Tickets.

Erweiterte Ticketfunktionen

Die erweiterten Ticketfunktionen hängen vom Tickettyp ab und stehen nur dem Ticketeigentümer zur Verfügung. Klicken Sie am unteren Ende des Formulars für Ticketeigenschaften auf "Erweitert", um auf die erweiterten Ticketeigenschaften zugreifen zu können.

Die meisten Tickets, die nicht informativ sind, verfügen über die folgenden Funktionen:

Kommentare hinzufügen

Klicken Sie, um dem Ticket einen Kommentar hinzuzufügen.

Anhänge hinzufügen

Klicken Sie, um dem Ticket einen Anhang hinzuzufügen.

Transaktionsprotokoll anzeigen

Klicken Sie, um das Transaktionsprotokoll des Tickets anzuzeigen.

Zusätzliche Funktionen, wie die Option, die Ticketinitiatoren, Verletzungen oder relevante Benutzer anzuzeigen, hängen vom Tickettyp ab.

Transaktionsprotokoll anzeigen

Das Transaktionsprotokoll enthält den Verlauf der mit Tickets in Verbindung stehenden Aktionen, die seit der Erstellung des Tickets ausgeführt wurden.

Die Tabelle "Transaktionsprotokoll anzeigen" enthält folgende Informationen:

Datum

Das Datum, an dem die Transaktion stattgefunden hat.

Benutzer

Vollständiger Benutzername:

Aktion

Typ der durchgeführten Aktion

Meldung

Eine vollständige Beschreibung der unternommenen Aktion.

So zeigen Sie das Transaktionsprotokoll der Kampagne an.

1. Klicken Sie am unteren Ende des Formulars für Ticketeigenschaften auf "Erweitert".
2. Klicken Sie auf "Transaktionsprotokoll anzeigen".

   Die Tabelle "Transaktionsprotokoll anzeigen" wird in einem separaten Browserfenster geöffnet.
3. Klicken Sie auf "Schließen", um das Popupfenster zu schließen.

TMS-Verwaltung

CA RCM implementiert Datenconnectorjobs und andere administrative Aufgaben mittels eines ticketbasierten Prozess-Management-Systems. Um auf globale Verwaltungs-Tools für das Ticket-Managementsystem (TMS) zuzugreifen, gehen Sie zu "Verwaltung", "Einstellungen", "TMS-Verwaltung".

Tickets bleiben im Allgemeinen im System und werden archiviert.

Wichtig! Wir empfehlen Ihnen dringend, Ihr System zu sichern, bevor Sie das Systemticket und die Tickettypen löschen.

Das TMS-Verwaltungs-Hilfsprogramm ermöglicht es Ihnen, das Folgende zu löschen:

- Alle Tickets
- Alle Tickettypen

Klicken Sie neben der Option, die Sie ausführen möchten, auf "Löschen". Nach der Löschung wird eine Bestätigungsmeldung angezeigt.

Import- und Exportconnectors

Connectors werden definiert, damit Benutzer und Benutzerberechtigungen (Entitäten und die Links zwischen ihnen) von Unternehmenssystemen in CA RCM importiert und exportiert werden können. Am Ende eines Auditprozesses vergleicht CA RCM die ursprüngliche Konfiguration, die aus einem Endpunkt importiert wurde, mit der neuen Konfiguration. CA RCM wendet dann Änderungen an, die sich aus der Implementierung der Unternehmensrichtlinien und Compliance-Regelungen auf die Konfigurationsabweichung zwischen der ursprünglichen und der aktualisierten Konfiguration ergeben. Die sich daraus ergebende Konfiguration wird unter Verwendung von Exportconnectors wieder zum Endpunkt exportiert.

Wo der Import und Export ausgeführt wird, hängt vom Connectortyp ab, den Sie verwenden. Das CA RCM-Portal ermöglicht es Ihnen, die folgenden Import- oder Exportconnectors zu definieren:

- Importconnectors
  - Benutzerdefinierte ausführbare Datei
  - CA RCM-Konfigurationsdokument (CFG)
  - Generisches Feed (CSV)
  - Datenbankkonfiguration
  - Identity Manager
  - Pentaho-Datenintegration (PDI)
  - CA RCM-Client-Batch (SBT)

    Hinweis: Das Ausführen des CA RCM-Client-Batch (SBT)-Connectors vom Portal aus wird unter AIX und Linux nicht unterstützt.

    Hinweis: Auf einem Windows-Rechner erstellte Dateien mit der Erweiterung "cfg" können auf eine Linux-Rechner nicht importiert importiert werden.
- Exportconnectors
  - Benutzerdefinierte ausführbare Datei
  - Datenbankkonfiguration
  - Identity Manager

Hinweis: Connectors werden explizit entweder als Importconnectors oder Exportconnectors definiert.

Einige Benutzer und Benutzerberechtigungen müssen direkt in CA RCM importiert werden, unter der Verwendung der Option "Importieren" im CA RCM Data Management (DM)-Client-Tool. Die Importoption aktiviert den Import aus den folgenden Endpunkten:

- Import
  - CSV-Dateien
  - LDIF-Dateien
  - Active Directory
  - RACF
  - TSS
  - UNIX
  - SAP
  - Freigegebener Windows-Ordner
  - ITIM
  - SA steuern
- Export
  - Active Directory
  - RACF
  - SQL-Datenbank
  - CSV-Dateien
  - ITIM V4.5 und V4.6
  - SA steuern

Hinweis: Weitere Informationen finden Sie im *DNA Data Management User Guide (DNA-Datenmanagement-Benutzerhandbuch)*.

Wichtig! Einige Connectors sind sowohl im CA RCM-Portal als auch im CA RCM Data Management-Client-Tool vorhanden. In diesen Fällen empfehlen wir, den Connector im CA RCM-Portal aus den folgenden Gründen auszuführen:

- Die Jobdefinition wird im Portal gespeichert, damit können Sie Import- und Exportaufgaben wiederholen.
- Abgerufene Daten werden direkt ins Universum integriert.

- Neue Daten können automatisch mit RACI-Definitionen der Konfiguration synchronisiert werden.
- Neue Benutzerdatensätze können automatisch mit Daten aus den Datensätzen der Personalabteilung oder anderer Quellen erweitert werden.

CA RCM-Connectors

Die folgenden *Import*-Connectors sind im CA RCM-Portal verfügbar:

Benutzerdefinierte ausführbare Datei

Ermöglicht es Ihnen, ein Skript oder eine ausführbare Datei in einer beliebigen Sprache (Perl, C++, C#, Java usw.) zu schreiben, um Daten in CA RCM zu importieren.

Die ausführbare Datei muss 7 CSV-Dateien erstellen (Users.udb, Resources.rdb, Roles.csv, UserRole.csv, UserResource.csv, RoleRole.csv, RoleResource.csv), und CA RCM importiert die Informationen aus jenen Dateien.

CA RCM-Konfigurationsdokument (CFG)

Liest die CA RCM-Datei, die einen Snapshot der Berechtigungen und Rollendefinitionen darstellt.

Hinweis: Auf einem Windows-Rechner erstellte Dateien mit der Erweiterung "cfg" können auf eine Linux-Rechner nicht importiert importiert werden.

Generisches Feed (CSV)

Liest CSV-Dateien als Eingabe, erstellt dann eine CA RCM-Konfiguration. Das CSV-Format (durch Kommas getrennte Werte) ist das üblichste Import- und Exportformat für Kalkulationstabellen und Datenbanken. CSV-Dateien können dann bei Bedarf mit einfachen Tools wie Excel bearbeitet und erweitert werden.

Das generische Feed verwendet sieben CSV-Dateien als Eingabe, wobei jede einzelne Datei einen Entitätstyp darstellt (wie Benutzerdatenbanken und Ressourcendatenbanken) oder eine Beziehung zwischen zwei Entitätstypen repräsentiert (Rollen). Einige Dateien sind optional und werden als leer angesehen, wenn sie beim Import nicht angegeben wurden. Der Connector erstellt eine Ausgabe-Datei, die die CA RCM-Konfigurationsdatei darstellt.

Datenbankkonfiguration

Ermöglicht den Import von Informationen aus einer CA RCM-Konfiguration (in der Datenbank) in die Master- und Modellkonfigurationen.

Identity Manager

Integriert CA RCM mit Identity Manager über die automatische Synchronisierung rollenbasierter Berechtigungen der zwei Systeme. Verwenden Sie den Connector, um Identity Manager-Daten zu importieren.

Weitere Informationen zum Connector für Identity Manager finden Sie im *Connector für Identity Manager-Handbuch*.

Pentaho-Datenintegration (PDI)

Ruft Transformationen und Jobs der Pentaho-Datenintegration (PDI) auf. Diese Funktion ermöglicht komplexe ETL-Operationen (Extrahieren, Transformieren und Laden) während des Datenimports. Um den PDI-Connector zu verwenden, legen Sie die Eigenschaft *pdi.home* auf den Pfad fest, an dem sich Ihr System befindet.

CA RCM-Client-Batch (SBT)

Führt die Batchverarbeitung aus. Sie müssen möglicherweise dynamische Parameter für Dateinamen angeben, die in den SBT-Dateien definiert sind.

Hinweis: Das Ausführen des CA RCM-Client-Batch (SBT)-Connectors vom Portal aus wird unter AIX und Linux nicht unterstützt.

Die folgenden *Export*-Connectors sind im CA RCM-Portal verfügbar:

Benutzerdefinierte ausführbare Datei

Ermöglicht es Ihnen, ein Skript oder eine ausführbare Datei in einer beliebigen Sprache (Perl, C++, C#, Java usw.) zu schreiben, um Daten aus CA RCM zu exportieren.

Die ausführbare Datei muss eine DIFF-Datei (siehe Seite 209)im DIFF-Dateiformat für CA RCM erstellen. CA RCM liest dann die DIFF-Datei und wendet die Änderungen an.

Datenbankkonfiguration

Ermöglicht den Export von Informationen aus einer CA RCM-Modellkonfiguration in eine andere Konfiguration in der Datenbank.

Identity Manager

Der Connector für Identity Manager ermöglicht Ihnen die Integration von CA RCM mit Identity Manager über die automatische Synchronisierung rollenbasierter Berechtigungen der zwei Systeme. Verwenden Sie den Connector, um aktualisierte Daten von CA RCM nach Identity Manager zu exportieren.

Die DIFF-Datei

Wenn zwei Konfigurationen in CA RCM verglichen werden, ist eine der dabei generierten Dateien die DIFF-Datei. Die DIFF-Datei identifiziert die Änderungen, die in einer Konfiguration auftreten, und ist die Grundlage für alle benutzerdefinierten ausführbaren (siehe Seite 207) Connectors.

Jede Zeile in einer DIFF-Datei identifiziert einen Unterschied. Die folgende Tabelle zeigt Beispielszeilen aus einer CA RCM-DIFF-Datei, mit einer Erklärung dazu, was jede Zeile angibt:

Zeile in DIFF-Datei	Erklärung
DIFF,ORIGCFG,SQL://sa@marro31w7.eurekify_sdb/ConfigWithRoles.cfg	Die erste Zeile einer DIFF-Datei, die die ursprüngliche Konfiguration definiert, aus der die DIFF-Datei erstellt wurde.
DIFF,UPDCFG,SQL://sa@marro31w7.eurekify_sdb/ConfigWithRoles2.cfg	Die zweite Zeile einer DIFF-Datei, die die aktualisierte Konfiguration definiert, aus der die DIFF-Datei erstellt wurde.
DIFF,REMOVEDROLE,"RBR"	Eine Zeile, deren zweites Feld "REMOVEDROLE" ist, zeigt an, dass eine Rolle aus der Konfiguration entfernt wird. Das dritte Feld ist der Name der entfernten Rolle.
DIFF,REMOVEDROLERES,"RBR","e-mail","outlook","WinNT"	Eine Zeile, deren zweites Feld "REMOVEDROLERES" ist, zeigt an, dass eine Ressource aus einer Rolle entfernt wird. Das dritte Feld ist der Name der Rolle, und die folgenden Felder sind die Ressourcennamen.
DIFF,REMOVEDROLEUSER,"RBR","54672910"	Eine Zeile, deren zweites Feld "REMOVEDROLEUSER" ist, zeigt an, dass ein Benutzer aus einer Rolle entfernt wird. Das dritte Feld ist der Name der Rolle und das vierte Feld ist der Name des Benutzers.
DIFF,NEWROLE,"NewRole",DESCRIPTION:"New-Rolle Description",ORG:"IT",ORG2:"IT2",ORG3:"Coorporate",OWNER:"67762440",TYPE:"Org Role",REVIEWER:"",FILTER:"Organization=IT;",CREATE DATE:"Thu der 02. Dez. 11:12:09 2010",APPROVAL DATE:"Thu der 02. Dez. 11:11:29 2010",EXPIRATION DATE:"None"	Eine Zeile, deren zweites Feld "NEWROLE" ist, zeigt an, dass eine Rolle zu der Konfiguration hinzugefügt wird. Die folgenden Felder sind die Attribute der neuen Rolle.

Zeile in DIFF-Datei	Erklärung
DIFF,NEWROLEUSER,"NewRole","67283470"	Eine Zeile, deren zweites Feld "NEWROLEUSER" ist, zeigt an, dass ein Benutzer zu einer Rolle hinzugefügt wird. Das dritte Feld ist der Name der Rolle und das vierte Feld ist der Name des Benutzers.
DIFF,NEWROLERES,"NewRole","UG5AVEMGR","NT5AVE","WinNT"	Eine Zeile, deren zweites Feld "NEWROLERES" ist, zeigt an, dass eine Ressource zu einer Rolle hinzugefügt wird. Das dritte Feld ist der Name der Rolle, und die folgenden Felder sind die Ressourcennamen.
DIFF,NEWROLEROLE,"NewRole","ADMPUR"	Eine Zeile, deren zweites Feld "NEWROLEROLE" ist, zeigt an, dass eine Unterrolle zu einer Rolle hinzugefügt wird. Das dritte Feld ist der Name der übergeordneten Rolle und das vierte Feld ist der Name der untergeordneten Rolle.
DIFF,COMMONROLEDIFFFIELD,"ADMNMGR",DESCRIPTION,"Sage Role","A modified description"	Eine Linie, deren zweites Feld COMMONROLEDIFFFIELD ist, zeigt an, dass eine Rolle aktualisiert wird. Die folgenden Felder sind die Attribute, die aktualisiert wurden.
DIFF,COMMONUSERNEWRES,"84774660","Domain Users","NTSTAM","WinNT"	Eine Zeile, deren zweites Feld "COMMONUSERNEWRES" ist, zeigt an, dass eine Ressource zu einem Benutzer hinzugefügt wird. Das dritte Feld ist der Name des Benutzers, und die folgenden Felder sind die Ressourcennamen.
DIFF,COMMONUSERREMOVEDRES,"99883110","\\Documents\\Employees","NT5AVE","WinNT"	Eine Zeile, deren zweites Feld "COMMONUSERREMOVEDRES" ist, zeigt an, dass eine Ressource aus einem Benutzer entfernt wird. Das dritte Feld ist der Name des Benutzers, und die folgenden Felder sind die Ressourcennamen.

Definieren von Connectors im CA RCM-Portal

Definieren Sie über das Fenster "Connectoreinstellungen" Import- und Exportconnectors im CA RCM-Portal. Das Fenster "Connectoreinstellungen" bietet die folgenden zwei Connectortabellen:

- Importe
- Exporte

Jede Tabelle zeigt eine Liste der verfügbaren Connectors an und bietet die Optionen, einen Connector zu bearbeiten, zu löschen, auszuführen oder zu planen. Die Schaltfläche "Neu hinzufügen", die über jeder Tabelle zu finden ist, ermöglicht es Ihnen, einen neuen Importconnector oder Exportconnector zu konfigurieren.

Definieren von Importconnectors

CA RCM-Importconnectors importieren Daten aus Endpunktsystemen.

Hinweis: Weitere Informationen finden Sie im *DNA Data Management User Guide (DNA-Datenmanagement-Benutzerhandbuch).*

So definieren Sie neue Importconnectors

1. Melden Sie sich am CA RCM-Portal als Administrator an.
2. Wechseln Sie zu "Verwaltung", "Einstellungen".

   Die Liste der verfügbaren Optionen wird angezeigt.
3. Klicken Sie auf "Connectoreinstellungen".

   Das Fenster "Connectoreinstellungen" wird geöffnet.
4. Klicken Sie über der Tabelle "Importe" auf "Neu hinzufügen".

   Das Fenster "Neuen Import hinzufügen" wird angezeigt.
5. Geben Sie im Abschnitt "Workflow-Informationen" die folgenden Informationen für den Connector an:

   Name des Importclients

   Geben Sie einen Namen für den Importconnector an.

   Beschreibung

   Gibt eine Beschreibung des Importconnectors an, wie die Verwendung, zeitliche Steuerung usw. des Connectors.

Universum

Gibt das Universum an, das sich mit dem Importconnector verknüpft ist. Die über diesen Connector erhaltenen Daten werden in die Masterkonfigurationsdateien des Universums importiert. Wenn es ein erstmaliger Import ist und keine Konfigurationsdateien vorhanden sind, erstellt der Importprozess die Konfigurationsdateien.

Hinweis: Bevor Sie einen Connectorjob ausführen können, legen Sie explizit ein Anmeldefeld für das Universum fest und stellen Sie sicher, dass der Connector die Endpunktdaten diesem Feld zuweist (siehe Seite 218).

(Optional) Erweiterungsbenutzerdatenbank

Definiert eine vorhandene Benutzerdatenbankdatei (.udb), die von CA RCM zur Erweiterung neuer Benutzerdatensätze beim Datenabruf verwendet wird. Daten werden aus einem bestimmten Endpunkt importiert, allerdings können Sie die ursprünglichen Daten erweitern, indem Sie zusätzliche Informationen aus einer zweiten Quelle hinzufügen. So können Sie zum Beispiel Benutzerinformationen von einem sicherheitsbezogenen Endpunkt herunterladen und dann die Daten erweitern, indem Sie auf zusätzliche Informationen einer Datenbank der Personalabteilung zugreifen. Diese Daten können Benutzeradressen beinhalten, die in der ersten Informationsquelle nicht vorhanden waren.

Hinweis: Geben Sie den Dateinamen ein, jedoch ohne das Suffix ".udb". Geben Sie zum Beispiel **Erweitern** ein, um auf die Datei "Erweitern.udb" zu verweisen.

Ticketvorlage

Gibt das Ticketformat an, das verwendet wird, um den Job in Ihrem Posteingang zu verfolgen. Wählen Sie "FlowTicketforImport_V0.8." aus.

Name des Workflow-Prozesses

Gibt den Workpoint-Geschäftsprozess an, den CA RCM verwendet, um den Connectorjob zu implementieren. Wählen Sie die "Konfiguration importieren" aus.

Maximale Dauer

Gibt eine geschätzte Verarbeitungszeit für den Job an. Wenn der Job jenseits dieser Frist weiterhin ausgeführt wird, listet CA RCM den Job in Ihrem Posteingang als überfällig auf, fährt jedoch mit der Bearbeitung fort.

Priorität

Gibt die Bedeutung des auf andere Aufgaben in Ihrem Posteingang bezogenen Jobs an.

Schweregrad

Gibt die Bedeutung der Fehler an, die bei der Bearbeitung der Jobs generiert wurde, und sich auf andere Aufgaben in Ihrem Posteingang beziehen.

6. Wählen Sie im Abschnitt "Connectorinformationen" den Connectortyp aus und geben Sie Werte für alle Eigenschaften an, die angezeigt werden. Neben jeder Eigenschaft werden weitere Informationen im Textformat angezeigt.
7. Klicken Sie auf "Speichern".

   Der Importconnector wurde definiert und wird jetzt in der Tabelle "Importe" angezeigt.

Erweiterungsbenutzerdatenbank

Beim Import von Daten können Sie über CA RCM Informationen in die leeren Felder neuer Benutzerdatensätze hinzufügen. Daten zum Personalwesen oder andere organisatorische Informationen können beispielsweise versendet werden, um neue Benutzerdatensätze zu erweitern.

Die Erweiterungswerte werden aus einer vorhandenen Benutzerdatenbank abgerufen. Um die Datenerweiterung zu implementieren, geben Sie die Datenbank an, wenn Sie den Connectorjob definieren. Die Daten in dieser Erweiterungsdatenbank überschreiben alle importierten Feldwerte.

Die folgende CA RCM-Systemeigenschaft kontrolliert diese Option.

hr.enrichment.clear_empty

Gibt an, wie sich leere Felder in der Anreicherungsdatenbank auf importierte Daten auswirken.

Wahr

Werte werden beim Datenimport unterdrückt, wenn das entsprechende Feld in der Anreicherungsdatenbank leer ist.

Falsch

Importierte Werte werden in die CA RCM-Zielkonfiguration geschrieben, wenn das entsprechende Feld in der Anreicherungsdatenbank leer ist.

hr.enrichment.clear_missing

Gibt an, wie sich fehlende Felder in der Anreicherungsdatenbank auf importierte Daten auswirken.

Wahr

Werte werden beim Datenimport unterdrückt, wenn das entsprechende Feld in der Anreicherungsdatenbank fehlt.

Falsch

Importierte Werte werden in die CA RCM-Zielkonfiguration geschrieben, wenn das entsprechende Feld in der Anreicherungsdatenbank fehlt.

Automatische RACI-Synchronisation

Der CA RCM-Server verwendet untergeordnete RACI-Konfigurationen (siehe Seite 272), um den Zugriff der Endbenutzer auf die Funktionen des CA RCM-Portals zu kontrollieren. Wenn Sie neue Benutzerdatensätze in eine Konfiguration importieren, können Sie diese neuen Benutzer automatisch in die RACI-Hierarchie dieser Konfiguration einschreiben.

Wenn ein importierter Benutzer keinen Anmeldenamen hat (Feld "Anmelde-ID" ist leer), hat er keinen Zugriff auf das CA RCM-Portal. Der automatische RACI-Synchronisationsprozess markiert diese Benutzer und benachrichtigt den Portaladministrator.

Definieren von Exportconnectors

CA RCM-Exportconnectors exportieren Daten in die Endpunktsysteme.

Hinweis: Weitere Informationen finden Sie im *DNA Data Management User Guide (DNA-Datenmanagement-Benutzerhandbuch).*

So definieren Sie Exportconnectors

1. Melden Sie sich am CA RCM-Portal als Administrator an.
2. Wechseln Sie zu "Verwaltung", "Einstellungen".

   Die Liste der verfügbaren Optionen wird angezeigt.
3. Klicken Sie auf "Connectoreinstellungen".

   Das Fenster "Connectoreinstellungen" wird geöffnet.
4. Klicken Sie über der Tabelle "Exporte" auf "Neu hinzufügen".

   Das Fenster "Neuen Export hinzufügen" wird angezeigt.

5. Stellen Sie die folgenden Informationen für den Connector zur Verfügung:

   Name des Exportclients

   Geben Sie einen Namen für den Exportconnector an.

   Beschreibung

   Gibt eine Beschreibung des Exportconnectors an, wie die Verwendung, zeitliche Steuerung usw. des Connectors.

   Universum

   Gibt das Universum an, das sich mit dem Exportconnector verknüpft ist.

   Hinweis: Bevor Sie einen Connectorjob ausführen können, legen Sie explizit ein Anmeldefeld für das Universum fest und stellen Sie sicher, dass der Connector die Endpunktdaten diesem Feld zuweist.

   Ticketvorlage

   Gibt das Ticketformat an, das verwendet wird, um den Job in Ihrem Posteingang zu verfolgen. Wählen Sie "FlowTicketforExport_V0.4." aus.

   Name des Workflow-Prozesses

   Gibt den Workpoint-Geschäftsprozess an, den CA RCM verwendet, um den Connectorjob zu implementieren. Wählen Sie eine der folgenden Optionen:

   - Master-Modell-Deltas mit Modell-Autokorrektur exportieren – Erstellt eine Auditkarte, die alle neuen Rollen enthält, die zur Reparation des Modells erstellt werden müssen. Nur in Verwendung mit Identity Manager-Connector.
   - Master-Modell-Deltas exportieren
   - Master-Modell-Deltas mit Modell-Korrektur exportieren – Erstellt ein Fehlerticket mit Links zur Auditkarte, wenn Fehler im Modell festgestellt werden. Nur in Verwendung mit Identity Manager-Connector.

   Maximale Dauer

   Gibt eine geschätzte Verarbeitungszeit für den Job an. Wenn der Job jenseits dieser Frist weiterhin ausgeführt wird, listet CA RCM den Job in Ihrem Posteingang als überfällig auf, fährt jedoch mit der Bearbeitung fort.

Priorität

Gibt die Bedeutung des auf andere Aufgaben in Ihrem Posteingang bezogenen Jobs an.

Schweregrad

Gibt die Bedeutung der Fehler an, die bei der Bearbeitung der Jobs generiert wurde, und sich auf andere Aufgaben in Ihrem Posteingang beziehen.

6. Wählen Sie den Connectortyp aus und geben Sie Werte für alle Eigenschaften ein, die unter Connectorinformationen angezeigt werden. Neben jeder Eigenschaft werden weitere Informationen im Textformat angezeigt.

7. Klicken Sie auf "Speichern".

   Der Exportconnector wurde definiert und wird jetzt in der Tabelle "Exporte" angezeigt.

Autokorrektur bei Export in Identity Manager

Der Exportprozess für Identity Manager wurde verbessert, um jetzt Fehler in der Modellkonfiguration automatisch zu beheben. Wenn ein Identity Manager-Connector erstellt wird, können Sie einen der folgenden neuen Workflow-Prozesse auswählen

- Master-Modell-Deltas mit Modell-Autokorrektur exportieren - Erstellt eine Auditkarte, die alle neuen Rollen enthält, die zur Korrektur des Modells erstellt werden
- Master-Modell-Deltas mit Modell-Korrektur exportieren - Wenn im Modell Fehler festgestellt werden, wird ein Fehlerticket mit Links zur Auditkarte erstellt.

Wenn Sie einen der beschriebenen Workflow-Prozesse auswählen, wird die folgende Logik auf CA RCM-Daten vor dem Export in Identity Manager angewendet:

- Wenn Sie eine Ressource mit einer Bereitstellungsrolle verbinden, ist die Ressource mit der Kontovorlage verbunden, die zur gleichen Bereitstellungsrolle auf dem Endpunkt gehört, auf dem sich die Kontovorlage befindet. Wenn keine Kontovorlage vorhanden ist, erstellt CA RCM eine Vorlage.
- Wenn eine übergeordnete Kontovorlage mit einer untergeordneten Bereitstellungsrolle verknüpft wird, wird die Linkrichtung umgekehrt.

- Wenn eine CA RCM-Rolle erstellt wird, wird der Typ folgendermaßen festgelegt:
  - Wenn der Rollentyp "Rolle" oder "Bereitstellungsrolle" ist, wird die Rolle als Bereitstellungsrolle exportiert.

    Der Rollentyp ist auf den Standardwert des Connectors festgelegt.

    Wenn die Rolle direkt verknüpfte Ressourcen hat, werden diese, wie bereits beschrieben, zu den verknüpften Kontovorlagen verschoben.
  - Wenn der Rollentyp "Richtlinie", "Bereitstellungsrichtlinie" oder "Konto-Vorlage" ist, wird die Rolle als Kontovorlage exportiert.

    Der Rollentyp ist auf den Standardwert des Connectors festgelegt.

    Wenn die Rolle mit keinem zulässigen Endpunkttyp anfängt, schlägt die Erstellung fehl und eine detaillierte Meldung wird angezeigt.

    Wenn die Rolle direkt verknüpfte Benutzer hat, schlägt die Ergänzung fehl und eine detaillierte Meldung wird angezeigt.

    Wenn die Rolle über Ressourcen verfügt, die nicht zum entsprechenden Endpunkttyp gehören, schlägt die Ergänzung fehl und eine detaillierte Meldung wird angezeigt.
  - Wenn eine Rolle keinen Typ hat, wird sie als Bereitstellungsrolle exportiert. Alle Details für diesen Export wurden weiter oben bereits beschrieben.

Ausführen und Planen von Connectorjobs

Sie können vordefinierte Connectorjobs ausführen, um Daten mit externen Systemen auszutauschen.

So planen Sie einen Connectorjob oder führen ihn aus

1. Legen Sie ein Anmeldefeld für das Universum fest (siehe Seite 218), und überprüfen Sie, ob der Connector diesem Feld Endpunktdaten zuweist.
2. Gehen Sie im CA RCM-Portal auf "Verwaltung", "Einstellungen" und klicken Sie auf "Connectoreinstellungen".

   Das Fenster "Connectoreinstellungen" wird geöffnet.

3. Führen Sie *einen* der folgenden Schritte aus:
   - Klicken Sie neben dem Connectorjob, den sie ausführen möchten, auf "Ausführen". Der Connectorjob wird sofort gestartet.
   - Planen Sie die zukünftige Ausführungen eines Connectorjobs wie folgt:
     a. Klicken Sie auf "Ablaufplan".

        Das Fenster "Aufgabe 'Neuer Connector geplant'" wird geöffnet.

     b. Füllen Sie die folgenden Felder aus:

     – Erste Ausführung – Gibt Datum und Uhrzeit für die erste Ausführung des Jobs an.

     – Anzahl der zusätzlichen Wiederholungen – Gibt die Anzahl der Ausführungen eines Jobs an. Geben Sie den Wert -1 ein, um eine unendliche Reihe festzulegen.

     – Wiederholungsintervall – Gibt den Zeitraum zwischen den Ausführungen der Jobs an.

     a. Klicken Sie auf "OK".

        Der Ablaufplan wird gespeichert und der Connectorjob wird zu den geplanten Zeitpunkten ausgeführt.

Überprüfen der Zuordnung des Anmeldefeldes

Wenn CA RCM neue auf Endpunktdaten basierte Benutzerdatensätze erstellt, werden automatisch Konten für diese Benutzer im CA RCM-Portal erstellt. Um dies zu unterstützen, muss der Connectorjob dem Anmeldefeld des Zieluniversums einen zulässigen Wert zuordnen.

So überprüfen Sie die Zuordnung des Anmeldefeldes

1. Überprüfen Sie, ob das Zieluniversum ein wie folgt festgelegtes Anmeldefeld hat:
   a. Gehen Sie im CA RCM-Portal auf "Verwaltung", "Einstellungen" und klicken Sie auf "Einstellungen des Universums".

      Das Fenster "Einstellungen des Universums" wird geöffnet.

   b. Suchen Sie das Universum, das Sie für den Connectorjob angegeben haben, und klicken Sie auf "Bearbeiten".

      Das Fenster "Bearbeiten" wird angezeigt:

c. Überprüfen Sie, ob sich das Anmeldefeld der Konfiguration auf ein vorhandenes Feld im Universum bezieht. Wenn das Anmeldefeld der Konfiguration leer ist, wählen Sie ein Feld aus.

d. Geben Sie den Namen des Anmeldefeldes der Konfiguration an.

2. Stellen Sie sicher, dass der Connector dem Anmeldefeld Daten wie folgt zuordnet:

   a. Öffnen Sie eine XML-Zuordnungsdatei, die Sie für den Connectorjob angegeben haben.

   b. Suchen Sie die Zeile, die dem Anmeldefeld zugewiesen ist. Die Zeile enthält den folgenden Begriff:

   ```
   host='Anmeldung'
   ```

   c. Überprüfen Sie, ob Endpunktdaten diesem Feld im **guest**-Begriff *zugeordnet sind.* Wenn diese Zuordnung leer ist, geben Sie ein Endpunktdatenfeld an.

Importieren und Exportieren von Tickets

Wenn ein Import oder Export fehlschlägt, generiert das CA RCM-Portal ein Fehlerticket.

Das Exportticket hat die folgenden Funktionen:

Schließen

Schließt das Ticket.

Speichern

Speichert alle Änderungen des Tickets.

Delegieren

Überträgt das Ticket an einen anderen Manager.

Eskalieren

Überträgt das Ticket an einen anderen Manager.

Bestätigen

Deaktiviert, bis der Vorgang abgeschlossen wurde. Klicken Sie auf diese Schaltfläche, um das Ticket zu vervollständigen und zu archivieren.

Verarbeiten

Stellt sicher, dass, auch wenn mehrere Benutzer dieses Fehlerticket erhalten, nur einer es auch wirklich bearbeitet. Nachdem ein Benutzer auf diese Schaltfläche geklickt hat, wird die Funktionsschaltfläche in den Tickets der restlichen Benutzer deaktiviert.

Job beenden

Der zurzeit ausgeführte Job kann manuell beendet werden.

(Nur für CA Identity Manager-Export) Beheben (siehe Seite 216)

Repariert den Job und fährt mit dem Export fort.

Bereinigen

Löscht die temporären Dateien, bevor der Job abgeschlossen wird.

Weitere Informationen:

Formular für Ticketeigenschaften (siehe Seite 201)

So definieren und führen Sie Multi-Import-Jobs aus

Sie können die Funktion "Multi-Import" verwenden, um mehrere Importjobs, die ein einziges Universum aktualisieren, zu gruppieren. Das Ergebnis ist ein einziger Job, der Daten aus mehreren Quellen importiert und sie in eine Konfigurationsdatei zusammenführt.

Ein Multi-Import-Job kann in zwei Schritten implementiert werden:

1. Definieren Sie einen Multi-Import-Job (siehe Seite 221) und alle entsprechenden Connectors im CA RCM-Portal.
2. Führen (siehe Seite 217) Sie diesen Multi-Import-Job aus oder planen Sie ihn mithilfe der Tools zur Jobplanung im CA RCM-Portal.

Wenn Daten aus mehreren Quellen in einem Multi-Import-Job zusammengeführt werden, wird die Datenzuordnung der verschiedenen Quellen angeglichen. Die resultierende Konfigurationsdatei stimmt möglicherweise nicht mit der Datenstruktur der vorhandenen Konfigurationen im Universum überein. Beachten Sie Folgendes:

- Wenn Sie einen Multi-Import-Job verwenden, um ein neues, leeres Universen aufzufüllen (siehe Seite 223), definiert die zusammengeführte Konfiguration die Standarddatenstruktur des Universums. Dieses Beispiel ist die häufigste Verwendung von Multi-Imports.
- Wenn Sie Multi-Import verwenden, um Daten in ein bereits vorhandenes Universum zu importieren, stellen Sie sicher, dass die Zuordnung aller Datenquellen untereinander und mit dem Universum übereinstimmen.

Definieren eines Multi-Import-Jobs

Sie können Multi-Import-Jobs im CA RCM-Portal definieren. Führen Sie diesen Job aus, um Daten aus mehreren Quellen automatisch zu importieren.

Beachten Sie Folgendes:

- Wenn mehrere Konfigurationsdateien als Datenquellen benutzt werden, müssen alle Dateien das gleiche Schema wie das Zieluniversum haben. Zum Beispiel müssen alle Dateien das gleiche Feld für die Personen-ID, E-Mail usw. verwenden.
- Multi-Import korreliert importierte Benutzerinformationen nicht von mehreren Datenquellen. Weitere Informationen zur Identifizierung wahrscheinlicher Übereinstimmungen, Überschneidungen und Duplikaten von mehreren Datenquellen finden Sie in der UUID-Dokumentation des *DNA Data Management User Guide (DNA-Datenmanagement-Benutzerhandbuch)*.

So definieren Sie Multi-Import-Jobs

1. Melden Sie sich am CA RCM-Portal als Administrator an.
2. Gehen Sie zu "Verwaltung", "Einstellungen" und klicken Sie auf "Multi-Import".

   Das Hauptfenster "Multi-Import" wird angezeigt.
3. Klicken Sie auf "Neue hinzufügen".

   Das Fenster "Multi-Import bearbeiten" wird angezeigt.
4. Geben Sie Werte für die Felder "Name" und "Beschreibung" des Multi-Import-Jobs ein.

5. Wählen Sie aus der Dropdown-Liste "Universum" das Universum aus, das aktualisiert werden soll.
6. Fügen Sie wie folgt eine Import-Aufgabe zum Multi-Import-Job hinzu:
   a. Wählen Sie den gewünschten Typ des Importjobs aus der Dropdown-Liste "Connector auswählen" zur Implementierung aus.
   b. Klicken Sie auf "Konfigurieren und zum Zusammenführen hinzufügen".

      Ein Konfigurationsfenster wird angezeigt. Es werden Felder für den von Ihnen ausgewählten Import-Job-Typ aufgelistet.
   c. Geben Sie Werte für alle angezeigten Connectoreigenschaften an.
   d. Klicken Sie auf "Fertig".

      Die neue Import-Aufgabe wird in der Tabelle angezeigt.
7. Wiederholen Sie Schritt 6 und definieren Sie beliebig viele Import-Aufgaben.
8. (Optional) Klicken Sie in der Zeile der Importaufgabe, die Sie entfernen möchten, auf "Löschen".
9. Legen Sie die Abschlussebene für den Job wie folgt fest:
   a. Klicken Sie oben rechts auf der Seite auf den Link "Gruppen verwalten".

      Das Fenster "Gruppen verwalten" wird angezeigt.
   b. Klicken Sie auf "Bearbeiten", um die Standardgruppe zu bearbeiten.

      Das Fenster "Gruppen" wird angezeigt.
   c. Bearbeiten Sie das Feld "Abschlussebene".

      Hinweis: Dieses Feld gibt den Prozentsatz der Import-Aufgaben an, die erfolgreich abgeschlossen werden müssen, damit der Multi-Import-Job als erfolgreich betrachtet wird. Wenn ein Multi-Import-Job zum Beispiel 20 Aufgaben enthält, und seine Abschlussebene auf 75 eingestellt ist, wird der Multi-Import-Job als erfolgreich betrachtet, wenn 15 dieser Aufgaben erfolgreich abgeschlossen wurden (15/20=75%). **Standard:** 100
   d. Klicken Sie zweimal auf "Speichern".

      Die Abschlussebene wird für den Job festgelegt, und das Multi-Import-Fenster wird angezeigt.
10. Klicken Sie im Fenster "Multi-Import bearbeiten" auf "Speichern".

    Das Hauptfenster für "Multi-Importe" wird angezeigt. Der neue Multi-Import-Job wird in der Multi-Import-Tabelle aufgelistet.

Verwenden von Multi-Import-Jobs, um leere Universen aufzufüllen

Ein Multi-Import-Job ermöglicht Ihnen, ein neues Universum mit CA RCM-Daten zu erstellen. Sie können einen einzelnen Job definieren und ausführen, der die folgenden Prozesse automatisiert:

- Datenimport aus mehreren Bereitstellungsknoten oder anderen Quellen
- Abstimmung von Feldzuordnung über Datenquellen
- Datenzusammenführungen aus verschiedenen Importconnectors
- Konfigurationsgenerierung mit einer optimalen Datenstruktur
- Auffüllen des Universums mit importierten Daten

Für den Multi-Import-Prozess werden Master- und Modellkonfiguration im Zieluniversum erwartet. Wenn Sie einen Multi-Import-Job basierend auf einem leeren Universum ausführen, verwenden Sie das Vorgangsticket in Ihrem Posteingang, um die Dateien für die Master- und Modellkonfiguration zu erstellen.

So verwenden Sie Multi-Import-Jobs, um leere Universen aufzufüllen

1. Definieren Sie ein neues Universum im CA RCM-Portal. Geben Sie Dummy-Namen für die Master- und Modellkonfigurationen an. Verwenden Sie keine Namen von bereits vorhandenen Konfigurationen.
2. Definieren Sie einen Multi-Import-Job (siehe Seite 221) Wählen Sie das in Schritt 1 angegebene Universum aus.
3. Führen Sie den Job aus (siehe Seite 217).
4. Klicken Sie im Hauptmenü des CA RCM-Portals auf den Posteingang.

   Er enthält ein Multi-Import-Ticket und ein Ticket zur Fehlerbehandlung für den Multi-Import-Job.
5. Klicken Sie zweifach auf das Fehlerbehandlungsticket.

   Ein Dialogfeld "Formular für Ticketeigenschaften" wird angezeigt.
6. Öffnen Sie den Abschnitt "Mehr" im Formular. Die folgende Meldung wird angezeigt:

   ```
   Ergebnisse der Überprüfung, ob die Datenbank Master- und
   Modellkonfigurationen wie im Universum [Universum_Name] definiert, enthält:
   Masterkonfiguration [Master_Name] - Nicht in der Datenbank vorhanden,
   Modellkonfiguration [Model_Name] - Nicht in der Datenbank vorhanden
   ```

   Hinweis: *Universum_Name, Master_Name,* und *Modell_Name* sind die Namen, die Sie bei der Definition des neuen Universums angegeben haben.

7. Klicken Sie auf "Bearbeiten".

   Die Schaltfläche "Universum erstellen" wird angezeigt.

8. Klicken Sie auf "Universum erstellen".

   Das Problem ist damit behoben.

9. Kehren Sie zum Posteingang zurück und +klicken Sie auf "Aktualisieren".

   In der Warteschlange wird ein neues Fehlerbehandlungsticket aufgelistet.

10. Klicken Sie zweifach auf das Fehlerbehandlungsticket.

    Ein Dialogfeld "Formular für Ticketeigenschaften" wird angezeigt.

11. Öffnen Sie den Abschnitt "Mehr" im Formular. Die folgende Meldung wird angezeigt:

    ```
    Vergleich der Universum-Masterkonfiguration mit der
    Berechtigungskonfiguration fehlgeschlagen. Das Universum [Universum_Name] hat
    keine Zuordnung für das Feld "Anmelde-ID", gehen Sie zu Verwaltung >
    Einstellungen > Einstellungen des Universums und ordnen Sie das Feld
    "Anmelde-ID" zu.
    ```

12. Klicken Sie auf "Bearbeiten".

    Die Schaltfläche "Synchronisation überspringen" wird angezeigt.

13. Klicken Sie auf "Synchronisation überspringen".

    Das Problem ist damit behoben. Der Multi-Import-Job wird fortgesetzt.

    Hinweis: Sie können das Multi-Import-Ticket öffnen, um den Fortschritt des Jobs zu überwachen.

Workflow- und Kampagnenverwaltung

Definieren von Tabellenformaten für das Übersichtsfenster "Meine Aufgaben"

Sie können das Tabellen-Layout anpassen, das verwendet wird, um in den Warteschlangen "Meine Aufgaben" von teilnehmenden Prüfern Gruppen von Workflow-Aktionen anzuzeigen.

Obligatorische Spalten können nicht aus Tabellenansichten entfernt werden. Roter Text und ein gesperrtes Schlosssymbol zeigen obligatorische Spalten in Benutzeranpassungsfenstern und Dialogfeldern an. Einige obligatorische Spalten sind hartkodierte Standards in CA RCM. Administratoren können zusätzliche obligatorischen Spalten definieren.

Gehen Sie folgendermaßen vor, um Standard-Tabellen-Layouts für das *Übersichtsfenster* "Meine Aufgaben" zu definieren.

Hinweis: Sie gehen anders vor, um Standard-Tabellenlayouts für *Aktionsdetailsfenster* in der Warteschlange "Meine Aufgaben" zu definieren.

So definieren Sie Tabellenformate für das Übersichtsfenster "Meine Aufgaben"

1. Gehen Sie im CA RCM-Portal auf "Verwaltung", "Workflow-Einstellungen", "Einstellungen der Inbox-Anzeige im Workflow".

   Das Fenster "Einstellungen der Inbox-Anzeige im Workflow" enthält vier Tabellenköpfe. Die Köpfe "Allgemeine Aufgaben", "Benutzeraufgaben", "Rollenaufgaben" und "Ressourcenaufgaben" zeigen die Tabellenlayouts, die verwendet werden, um im Übersichtsfenster "Meine Aufgaben" Gruppen von Aktionen anzuzeigen.

2. Passen Sie das Tabellen-Layout folgendermaßen an:

   a. Klicken Sie auf dem Tabellenkopf, den Sie ändern wollen, auf "Anpassen".

      Das Dialogfeld "Anpassen" wird angezeigt.

   b. Verwenden Sie die Pfeiltasten, um Spalten hinzuzufügen oder zu entfernen, und um die Spalten anzuordnen.

   c. Wenn Sie die Spalten angepasst haben, klicken Sie auf OK.
   d. Klicken Sie auf das Sperrsymbol neben dem Spaltennamen, um die Spalte obligatorisch zu machen. Benutzer können eine obligatorische Spalte verschieben, können sie jedoch nicht entfernen.

      Hinweis: Obligatorische Spalten werden in Rot angezeigt.

3. Klicken Sie auf "Änderungen übernehmen".

   CA RCM zeigt Gruppen von Benutzeraktionen in den Tabellenformaten an, die Sie angegeben haben.

Optionen für Standard-Workflow-Aktionen

Sie können die Tools steuern, die für Geschäftsteilnehmer zur Verfügung stehen, wenn sie Aktionen in ihrer Warteschlange "Meine Aufgaben" bearbeiten, oder wenn sie Geschäfts-Workflows in ihrer Warteschlange "Meine Anforderungen" verwalten. Die folgenden Systemeigenschaften aktivieren optionale Steuerelemente in diesen Fenstern.

Hinweis: Diese Eigenschaften wirken sich auch auf die von CA RCM-Administratoren verwendeten Workflow-Verwaltungs-Fenster aus.

Die folgenden Systemeigenschaftsteuerelemente gruppieren die Bearbeitung von Aktionen in Aktionsdetailsfenstern:

businessflows.reviewers.default.allowSelectAll

Bestimmt, ob Prüfer alle Aktionen in einer Tabelle als Gruppe verarbeiten können. Wenn diese Boolesche Eigenschaft wahr ist, haben Aktionsdetailtabellen Kontrollkästchen in den Kopfzeilen "Genehmigen", "Ablehnen" und "Neu zuweisen". Prüfer wählen diese Kontrollkästchen an, um eine Entscheidung für alle Links in der Tabelle zu treffen. Diese Eigenschaft bestimmt auch das Standard-Verhalten für Kampagnen: wenn diese Eigenschaft wahr ist, wird die Spalte "Ermöglichen Sie Managern, eine ganze Spalte auszuwählen" im Assistenten "Kampagne hinzufügen" standardmäßig ausgewählt.

Die folgenden Systemeigenschaften erlauben es Benutzern, Gruppen von Aktionen vom Übersichtsfenster "Meine Aufgaben" aus zu bearbeiten.

businessflows.inbox.approveRejectAll.enabled

Bestimmt, ob Prüfer Gruppen von Aktionen im Übersichtsfenster "Meine Aufgaben" genehmigen oder ablehnen können. Wenn diese Boolesche Eigenschaft wahr ist, zeigt das Übersichtsfenster "Meine Aufgaben" die Spalten "Zuweisen" und "Ablehnen". Benutzer können im Fenster aufgelistete Gruppen von Aktionen genehmigen oder ablehnen. Sie können auch in den Kopfzeilen der Spalten "Genehmigen" und "Ablehnen" die Kontrollkästchen anwählen, um eine Entscheidung auf alle Inhalte einer Tabelle anzuwenden.

businessflows.inbox.reassignAll.enabled

Bestimmt, ob Prüfer Gruppen von Aktionen im Übersichtsfenster "Meine Aufgaben" neu zuweisen können. Wenn diese Boolesche Eigenschaft wahr ist, zeigt das Übersichtsfenster "Meine Aufgaben" die Spalte "Neu zuweisen". Benutzer können Gruppen von aufgelisteten Aktionen im Fenster neuzuweisen. Sie können auch im Spaltenkopf "Neu zuweisen" Kontrollkästchen aktivieren, um sämtliche Inhalte einer Tabelle neuzuzuweisen.

Weitere Informationen:

Aktivierung der Gruppenüberprüfung von Aktionen (siehe Seite 82)
Neu zuweisen von Links an andere Prüfer (siehe Seite 53)

So passen Sie das E-Mail-Verhalten an

Standardmäßig sendet der CA RCM-Server E-Mails in verschiedenen Etappen einer Zertifizierungskampagne sowie für Self-Service-Anforderungen. Diese E-Mails verwenden eine Reihe von im Server gespeicherten Vorlagen.

Sie können dieses Verhalten auf verschiedene Weisen anpassen:

- Sie können angepasste Vorlagen erstellen, die zusätzliche Erklärungen oder für Ihre Organisation spezifische Kommentare enthalten.
- Sie können E-Mails standardmäßig für bestimmte Ereignisse deaktivieren.

Wenn Sie eine Zertifizierungskampagne erstellen, können Sie E-Mails für jedes Ereignis der Kampagne aktivieren oder deaktivieren und angeben, welche Vorlage für jeden Typ von E-Mail verwendet wird.

Erstellen einer benutzerdefinierten E-Mail-Vorlage

Sie können Vorlagen anpassen, um zusätzliche Erklärungen oder Kommentare zu Ihrer Organisation oder zu bestimmtem Geschäftsszenarien einzuschließen. Zum Beispiel können Sie eine Reihe von E-Mail-Vorlagen für die Zertifizierung von Benutzerberechtigungen durch direkte Manager erstellen, und eine weitere Reihe von Vorlagen für die Rezertifizierung durch Manager auf höherer Ebene. Sie wählen aus, welche Vorlagen zu verwenden sind, wenn Sie eine Kampagne erstellen.

Vorlagen können zur Einfügung persönlicher Daten Parameterfelder verwenden, ähnlich einer Seriendruckeinrichtung.

E-Mail-Aggregation konsolidiert mehrere E-Mail-Anfragen des gleichen Typs, die an ein und dieselbe Person gerichtet sind. Zum Beispiel: In einer Kampagne zur Benutzerzertifizierung zertifiziert ein Manager die Berechtigungen all seiner Arbeiter. Die Kampagne generiert mehrere Überprüfungsaktions-E-Mails an den Manager, eine pro Mitarbeiter. CA RCM konsolidiert diese E-Mail-Anfragen, und sendet dem Manager eine einzige E-Mail.

Ziehen Sie bei der Erstellung einer E-Mail-Vorlage die Möglichkeit einer Aggregation in Betracht. Die gleiche Vorlage wird für eine oder mehrere Aktionen verwendet.

Es wird empfohlen, dass Sie für die erste Vorlage, die Sie für ein E-Mail-Auslöseereignis anpassen, von der für dieses Ereignis angegebenen Standard-CA RCM-Vorlage (siehe Seite 232) ausgehen.

So erstellen Sie eine benutzerdefinierte E-Mail-Vorlage

1. Gehen Sie im CA RCM-Portal auf "Verwaltung", "Einstellungen", "E-Mail", "Vorlagen".

   Das E-Mail-Vorlagen-Fenster wird angezeigt.

2. (Empfohlen) Um die neue Vorlage anhand einer vorhandenen Vorlage für den E-Mail-Auslöser zu erstellen:

   a. Klicken Sie auf "Laden".

      Das Dialogfeld "Neue Vorlage" wird geöffnet.

   b. Wählen Sie eine vorhandene Vorlage aus der Drop-down-Liste "Auswählen", und klicken Sie auf OK.

      Die vorhandene Vorlage wird in einem Bearbeitungsfenster angezeigt. Die Schaltfläche "Spechern" ist nicht verfügbar.

   c. Klicken Sie auf "Speichern als" und benennen die Vorlage um.

3. Um mit einer neuen, unbeschriebenen Vorlage zu beginnen:
    a. Klicken Sie auf "Neu".

       Das Dialogfeld "Neue Vorlage" wird geöffnet.
    b. Wählen Sie aus der Drop-down-Liste "E-Mail-Ereignis" das Auslöseereignis aus, das diese Vorlage verwendet.
    c. Geben Sie einen Namen für die Vorlage an.
    d. Klicken Sie auf "OK".

       Das Vorlagenbearbeitungsfenster öffnet sich.
4. Bearbeiten Sie den Vorlagentext.
5. (Optional) Um ein Parameterfeld hinzuzufügen:
    a. Bewegen Sie in den Bereichen "Betreff" oder "Text" den Cursor an die Stelle, an der Sie das Feld einfügen möchten.
    b. Suchen Sie den Parameter in der Parameterliste unter dem Vorlagenbearbeitungsfenster.
    c. Klicken Sie neben dem Feld auf "Dem Betreff hinzufügen" oder "Dem Text hinzufügen".

    Der Parameter wird in die Vorlage eingefügt. Wenn E-Mails versendet werden, wird der Parameter durch tatsächliche Daten ersetzt.
6. (Optional) Verwenden von HTML-Code im Vorlagentext. (siehe Seite 230)
7. Klicken Sie zum Speichern der Vorlage auf "Speichern".

HTML-Elemente in E-Mail-Vorlagen

Sie können HTML-Elemente in E-Mail-Vorlagen einfügen, um Hyperlinks hinzuzufügen oder Text zu formatieren. Da CA RCM die Vorlage in eine E-Mail mit HTML-Formatierung konvertiert, müssen Sie HTML-Elemente in <html>-Tags einschließen. CA RCM fügt Inhalt innerhalb der <html>-Tags direkt in den E-Mail-Text ein.

E-Mail-Vorlagen unterstützen keine Stylesheets und kein JavaScript.

Hinweis: Wenn Sie einen Lotus Notes-E-Mail-Client verwenden, können in einer HTML-Vorlage Probleme mit dem
-Tag auftreten. Die Probleme treten auf, weil CA RCM dem
-Tag standardmäßig einen Schrägstrich (/) hinzufügt:
. Um diese Probleme zu vermeiden, fügen Sie unter "Verwaltung", "Einstellungen", "Eigenschaftseinstellungen", die folgende Systemeigenschaft hinzu:

html.linebreak

Legen Sie den Wert der Eigenschaft auf
 fest.

Sobald diese Eigenschaft festgelegt ist, können Sie
 in
 umändern.

Beispiel: Einfügen eines Hyperlinks

Der folgende Code in einer Vorlage erstellt Hyperlinks zu Informationsseiten auf der CompanyWeb-Website:

```
Weitere Informationen:
<html>
<A href="http://CompanyWeb.com/Certfication.html">Was ist eine
Zertifizierungskampagne?</a><br>
<A href="http://CompanyWeb.com/RBAC.html">Was ist rollenbasierte
Zugriffskontrolle?</a>
</html>
```

Der Code generiert die folgenden Hyperlinks in den E-Mails, die an die Benutzer gesendet werden:

```
Weitere Informationen:
Was ist eine Zertifizierungskampagne?
Was ist rollenbasierte Zugriffskontrolle?
```

E-Mails aktivieren und eine Vorlage zuweisen

Verschiedene Ereignisse lösen E-Mails aus. Sie können E-Mails für ein Ereignis deaktivieren oder eine benutzerdefinierte Vorlage für von diesem Ereignis ausgelöste E-Mails zuweisen.

Sie müssen eine benutzerdefinierte Vorlage (siehe Seite 228) erstellen, bevor Sie sie einem Ereignis zuweisen können.

Hinweis: Sie benötigen Administrator-Berechtigungen im CA RCM-Portal, um diesen Vorgang auszuführen.

So aktivieren Sie E-Mails weisen eine Vorlage zu

1. Klicken Sie im CA RCM-Portal auf "Verwaltung", "Einstellungen", "E-Mail", "Ereignisse".

   Das Fenster "E-Mail-Ereignisse" zeigt eine Liste von Ereignissen an, die E-Mails auslösen.

   Hinweis: Dieses Fenster zeigt ältere Ereignise und Vorlagen von Vorgängerversionen von CA RCM an. Ereignisse von Vorgängerversionen werden ganz oben in der Tabelle aufgelistet und haben gesonderte Aggregationsvorlagen. Aktivieren Sie diese Ereignisse nicht.

2. Wählen Sie die Ereignisse aus, für die Sie E-Mails auslösen wollen. Löschen Sie Ereignisse, für die Sie keine E-Mails auslösen möchten.

3. (Optional) Wählen Sie in der Drop-down-Liste "Vorlage" des Ereignisses eine alternative Vorlage für das Ereignis aus.

4. Klicken Sie auf "Speichern", um die Einstellungen zu speichern.

   Die ausgewählten Ereignisse werden aktiviert und die Vorlagen werden zugewiesen.

Standard-E-Mail-Vorlagen

CA RCM bietet die folgenden Standard-E-Mail-Vorlagen:

Kampagnenaufgaben neu zuweisen

Wird an den Benutzer gesendet, der eine neu zugewiesene Zertifizierungsaufgabe übernimmt.

Standardvorlagen: CampaignReassignDefault, Agg.CampaignReassignDefault

Kampagneneskalations-E-Mail

Wird gesendet, wenn der Kampagneneigentümer Eskalations-E-Mails initiiert.

Standardvorlagen: ApproverDefault, Agg.ApproverDefault, ManagerDefault, Manager2-Standard, Manager3-Standard

Benutzerkampagne starten

Wird an einen Benutzer gesendet, der eine Kampagne zur Benutzerzertifizierung erstellt.

Standardvorlagen: UserCampaignNotificationDefault, Agg.UserCampaignNotificationDefault

Rollenkampagne starten

Wird an einen Benutzer gesendet, der eine Kampagne zur Rollenzertifizierung erstellt.

Standardvorlagen: RoleCampaignNotificationDefault, Agg.RoleCampaignNotificationDefault

Ressourcenkampagne starten

Wird an einen Benutzer gesendet, der eine Kampagne zur Ressourcenzertifizierung erstellt.

Standardvorlagen: ResourceCampaignNotificationDefault, Agg.ResourceCampaignNotificationDefault

Kampagneneinstellungen erfolgreich abgeschlossen

Wird an den Verantwortlichen einer Kampagne gesendet, wenn die Kampagnenerstellung erfolgreich war.

Standardvorlage: CampaignSettingsCompletdSuccDefault

Kampagneeinstellungenen nicht erfolgreich abgeschlossen

Wird an den Verantwortlichen einer Kampagne gesendet, wenn die Kampagnenerstellung nicht erfolgreich war.

Standardvorlage: CampaignSettingsCompletdUnsuDefault

Importprozess - Keine Anmeldung für einige Benutzer

Wird gesendet, wenn ein Importprozess neue Benutzerdatensätze identifiziert, die keinen Wert in dem für das Zieluniversum angegebenen Benutzeranmeldungsfeld besitzen.

Standardvorlage: ImportUsersNoLoginWarningDefault

Neue Kampagnenzertifizierungsaufgabe

Wird gesendet, wenn eine Kampagne vorbereitende Zertifizierungsüberprüfungsaufgaben generiert.

Standardvorlage: CertificationOpenCertifyUserActionDefault

Neue Kampagnengenehmigungsaufgabe

Wird gesendet, wenn eine Kampagne Änderungsgenehmigungsüberprüfungsaufgaben für vorhandene Links generiert.

Standardvorlage: CertificationOpenApproveUserActionDefault

Neue Kampagnenvorschlagsaufgabe

Wird gesendet, wenn eine Kampagne vorbereitende Zertifizierungsaufgaben für vorgeschlagene Links generiert.

Standardvorlage: CertificationOpenSuggestUserActionDefault

Neue Kampagnenkonsultierungsaufgabe

Wird gesendet, wenn ein Prüfer sich mit anderen Prüfern in einer Kampagne berät.

Standardvorlage: CertificationOpenConsultUserActionDefault

Neu zugewiesene Kampagnenzertifizierungsaufgabe

Wird gesendet, wenn ein Prüfer die vorbereitenden Zertifizierungsüberprüfungsaufgaben in einer Kampagne neu zuweist.

Standardvorlage: CertificationReassignCertifyUserActionDefault

Neu zugewiesene Kampagnengenehmigungsaufgabe

Wird gesendet, wenn ein Prüfer die Genehmigungsänderungsüberprüfungsaufgaben in einer Kampagne neu zuweist.

Standardvorlage: CertificationReassignApproveUserActionDefault

Neu zugewiesene Kampagnenvorschlagsaufgabe

Wird gesendet, wenn ein Prüfer die vorbereitenden Zertifizierungsüberprüfungsaufgaben für vorgeschlagene Links in einer Kampagne neu zuweist.

Standardvorlage: CertificationReassignSuggestUserActionDefault

Neu zugewiesene Kampagnenberatungsaufgabe

Wird gesendet, wenn ein Prüfer die Konsultierungsüberprüfungsaufgaben in einer Kampagne neu zuweist.

Standardvorlage: CertificationReasssignConsultUserActionDefault

Neue Genehmigungsaufgabe

Wird gesendet, wenn CA RCM Genehmigungsaufgaben für Änderungen an der Modellkonfiguration generiert.

Standardvorlage: ApprovalOpenApproveUserActionDefault

Neue Genehmigungskonsultierungsaufgabe

Wird gesendet, wenn CA RCM Konsultierungsüberprüfungsaufgaben für Änderungen an der Modellkonfiguration generiert.

Standardvorlage: ApprovalOpenConsultUserActionDefault

Neu zugewiesene Genehmigungaufgabe

Wird gesendet, wenn ein Prüfer Genehmigungsaufgaben für Änderungen an der Modellkonfiguration neu zuweist.

Standardvorlage: ApprovalReassignApproveUserActionDefault

Neu zugewiesene Genehmigungskonsultierungsaufgabe

Wird gesendet, wenn ein Prüfer Konsultierungsüberprüfungsaufgaben für Änderungen an der Modellkonfiguration neu zuweist.

Standardvorlage: ApprovalReassignConsultUserActionDefault

Neue Self-Service-Genehmigungsaufgabe

Wird gesendet, wenn CA RCM Genehmigungsaufgaben für Self-Service-Anfragen generiert.

Standardvorlage: SelfServiceOpenApproveUserActionDefault

Neue Self-Service-Genehmigungskonsultierungsaufgabe

Wird gesendet, wenn CA RCM Genehmigungskonsultierungsaufgaben für Self-Service-Anfragen generiert.

Standardvorlage: SelfServiceOpenConsultUserActionDefault

Neu zugewiesene Self-Service-Genehmigungsaufgabe

Wird gesendet, wenn ein Prüfer Genehmigungsaufgaben für Self-Service-Anfragen neu zuweist.

Standardvorlage: SelfServiceReassignApproveUserActionDefault

Neu zugewiesene Self-Service-Genehmigungskonsultierungsaufgabe

Wird gesendet, wenn CA RCM Genehmigungskonsultierungsaufgaben für Self-Service-Anfragen generiert.

Standardvorlage: SelfServiceReassignConsultUserActionDefault

Fehler beim Versenden von E-Mails

Wird an den CA RCM-Administrator gesendet, wenn ein Versuch, eine E-Mail zu senden, fehlschlägt.

Standardvorlage: ErrorSendingEMail

email.event.title.noEvent

Für E-Mails an Benutzer, die keinen Zugriff auf das CA RCM-Portal haben.

Standardvorlage: BasicEmail

Systemeigenschaften für E-Mails

Verwenden Sie die folgenden Systemeigenschaften, um eine CA RCM-Verbindung zu einem SMTP-Server zu konfigurieren und das E-Mail-Verhalten zu definieren.

Hinweis: Einige dieser Eigenschaften werden während der CA RCM-Installation automatisch festgelegt.

mail.Server

Definiert die URL des <SMTP>-Servers.

mail.ServerPort

Definiert den für die Kommunikation mit dem SMTP-Server verwendeten Port.

mail.user

Definiert das CA RCM-Benutzerkonto auf dem SMTP-Server.

mail.password

Definiert das Kennwort des CA RCM-Kontos auf dem SMTP-Server.

mail.from

Definiert die ausgehende E-Mail-Adresse des CA RCM-Servers. **Standard:** RCM@ca.com

mail.useSSL

Bestimmt, ob die Kommunikation mit dem SMTP-Server SSL-Verschlüsselung verwendet.

mail.max.attempts

Definiert, wie oft CA RCM versucht, eine E-Mail zu senden.

mail.sending interval

Definiert die Zeit, in Sekunden, zwischen zwei Versuchen von CA RCM, E-Mails zu versenden.

portalExternalLink.inboxUrl

Definiert den Wert des inboxLink-Parameters in E-Mail-Vorlagen. Dies ist eine allgemeine Ziel-URL auf dem CA RCM-Server, die eines jeden Benutzers "Meine Aufgaben"-Warteschlange bedient.

Systemeigenschaften für Geschäfts-Workflows

Administratoren verwenden CA RCM-DNA und Datenverwaltungs-Client-Anwendungen, um CA RCM-Datendateien zu analysieren und direkt zu bearbeiten. Wenn die Administratoren eine Konfigurationsdatei ändern, können sie diese Änderungen an den CA RCM-Server senden. Der Server initiiert den entsprechenden Workflow, um die Änderungen zu genehmigen und zu implementieren.

Da kein Geschäftsteilnehmer diese Workflows initiiert, definieren die folgenden Systemeigenschaften eine Reihe von Standardeigentümern:

approvals.flowOwner

Definiert den Standardeigentümer von Workflows, die von CA RCM-Client-Anwendungen gesendet wurden. Standardmäßig ist der CA RCM-Systemadministrator der Eigentümer dieser Workflows. Um diese Eigenschaft für ein Universum zu implementieren, erstellen Sie eine Eigenschaft mit dem folgenden Namen:

`universe.property.`*`universe_name`*`.approvals.flowOwner`

Hinweis: "universe_name" ist der Name des Zieluniversums.

role.defaultOwner.enable

Bestimmt, ob die Systemeigenschaft "approval.role.defaultOwner" den Standardeigentümer für neue Rollenanforderungen von CA RCM-Client-Anwendungen definiert. Wenn diese Boolesche Eigenschaft falsch ist, ist der CA RCM-Eigentümer der Eigentümer dieser Rollen, und der Wert von approval.role.defaultOwner wird ignoriert.

approval.role.defaultOwner

Definiert den Standardeigentümer einer vorgeschlagenen neuen, von CA RCM-Client-Anwendungen gesendeten Rolle. Dieser Benutzer muss im Zieluniversum für Rollenerstellung sein. Wenn diese Eigenschaft null ist, oder wenn der angegebene Benutzer nicht im Zieluniversum ist, erstellt CA RCM die Rolle ohne einen Eigentümer. In diesem Fall überprüft der von der "approval.defaultManager"-Systemeigenschaft angegebene Benutzer die Rollenanforderung.

Planen von Jobs

Die Jobplanung ermöglicht es Ihnen, automatische und mehrmalige CA RCM-Jobs einzurichten. Jeder Job wird einem Universum zugewiesen und ein entsprechendes Ticket wird an den Posteingang des Administrators gesendet, wenn der Job abgeschlossen wurde.

Weitere Informationen zur Jobplanung finden Sie unter "Verwaltung" und "Jobplaner".

Ausführen oder Planen von Jobs im CA RCM-Portal

Sie können vordefinierte Connectorjobs oder andere Prozesse im CA RCM-Portal ausführen.

So führen Sie Jobs im CA RCM-Portal aus oder planen sie

1. Gehen Sie im CA RCM-Portal zu "Verwaltung" und danach auf "Jobplaner".
2. Suchen Sie den Job oder Prozess, den Sie ausführen möchten.
3. Führen Sie *einen* der folgenden Schritte aus:
   - Führen Sie den Job sofort aus, indem Sie in der Zeile des Prozesses auf "Ausführen" klicken.

     Der Job wird sofort gestartet.
   - Planen Sie einen oder mehrere zukünftige Jobs wie folgt:
     a. Klicken Sie in der Zeile des Prozesses auf "Ablaufplan".

        Das Dialogfeld "Aufgabe planen" wird angezeigt.
     b. Füllen Sie die folgenden Felder aus:

        Erste Ausführung – Gibt Datum und Uhrzeit der Initiierung des Jobs an.

        Zusätzliche Wiederholungen - Gibt die Anzahl der Jobinstanzen an, die sie generieren möchten. Geben Sie den Wert -1 ein, um eine unendliche Reihe von Jobs festzulegen.

        Wiederholungsintervall – Zeitraum zwischen den Jobs der Reihe.
     c. Klicken Sie auf "OK".

     Der Ablaufplan wird gespeichert. CA RCM initiiert Jobs automatisch nach Ablaufplan.

Die Jobtabelle

Die Jobtabelle führt alle Jobs auf, die in das System eingegeben wurden. Die Tabelle enthält die folgenden Felder:

Jobname

Gibt den Namen des Jobs an.

Beschreibung

Gibt eine Beschreibung zur Aufgabe des Job an.

Jobklasse

Listet die Java-Klasse des Jobs auf.

Startzeit

Geben Sie das Datum und die Uhrzeit an, zu der der Job startet.

Vorherige Ausführung

Wenn ein Job wiederholt wird, werden das Datum und die Uhrzeit der vorherigen Ausführung hier aufgeführt.

Nächste Ausführung

Gibt das Datum und die Uhrzeit an, wann der Job wiederholt werden soll.

Löschen

Ermöglicht Ihnen, Job zu löschen.

CA Enterprise Log Manager-Integration

Mit der CA Enterprise Log Manager-Integration können Sie CA Enterprise Log Manager-Nutzungsdaten in CA RCM importieren. CA RCM zeigt dann während Zertifizierungsüberprüfungen diese Nutzungsdaten an. Anwendungen in CA Enterprise Log Manager entsprechen Ressourcen in CA RCM. CA Enterprise Log Manager zeichnet den Benutzerzugriff auf eine Anwendung auf; CA RCM ruft diese Nutzungsdaten dann ab und zeigt sie während einer Kampagne an.

Bevor Sie beispielsweise den Benutzerzugriff auf eine Ressource (Anwendung) zertifizieren, können Sie die Nutzungsdaten daraufhin überprüfen, wie oft der Benutzer tatsächlich auf die Ressource zugreift.

Sie aktivieren die CA RCM-Integration mit CA Enterprise Log Manager einzeln pro Universum.

Führen Sie den folgenden Prozess aus, um die CA Enterprise Log Manager-Integration zu aktivieren.

1. Überprüfen Sie die Voraussetzungen für die Integration mit CA Enterprise Log Manager (siehe Seite 241).
2. Konfigurieren Sie die Kommunikation zwischen CA RCM und CA Enterprise Log Manager folgendermaßen:
    a. Importieren Sie CA RCM-Abfragen in CA Enterprise Log Manager.
    b. Erstellen Sie ein Sicherheitszertifikat für CA Enterprise Log Manager im Schlüsselspeicher des CA RCM-Servers.
    c. Registrieren Sie CA RCM auf dem CA Enterprise Log Manager-Server.
    d. Aktualisieren Sie CA RCM-Eigenschaften.
3. Ordnen Sie Daten zwischen CA RCM und CA Enterprise Log Manager folgendermaßen zu:
    a. Legen Sie das Anwendungsattribut im CA RCM-Universum fest.
    b. Ordnen Sie CA Enterprise Log Manager-Anwendungen den Anwendungen im CA RCM-Universum zu.
    c. Aktualisieren Sie Nutzungsdaten von CA Enterprise Log Manager auf CA RCM.
4. Um die Funktionseinstellungen zu bestätigen, öffnen Sie eine Konfiguration des Universums im Entitäten-Browser und überprüfen Sie, ob die Symbole zur Verwendung für Benutzer und Ressourcen angezeigt werden.

Voraussetzungen für die Integration mit CA Enterprise Log Manager

Bevor Sie CA RCM und CA Enterprise Log Manager für die Zusammenarbeit konfigurieren, vergewissern Sie sich, dass Folgendes zutrifft:

- Stellen Sie sicher, dass Sie über ein funktionierendes CA RCM-Universum mit importierten CA RCM-Entitäten verfügen. Wenn Sie in Ihrer Umgebung CA Identity Manager verwenden, wird die Kontokonfiguration automatisch erstellt. Wenn Sie CA Identity Manager nicht verwenden, müssen Sie die Kontoinformationen manuell in CA RCM importieren (siehe Seite 41).
- Installieren Sie CA Enterprise Log Manager und erstellen Sie einen Benutzer mit der Berechtigung, Ereignisse anzuzeigen.
- Erstellen Sie im Bedarfsfall Ereignisquellen (Anwendungen) in CA Enterprise Log Manager. Anwendungen entsprechen Ressourcen in CA RCM. CA Enterprise Log Manager zeichnet den Benutzerzugriff auf eine Anwendung auf; CA RCM ruft diese Nutzungsdaten dann ab und zeigt sie während einer Kampagne an.

  Hinweis: Weitere Informationen über die Erstellung von CA Enterprise Log Manager-Ereignisquellen finden Sie in der CA Enterprise Log Manager-Dokumentation.

Importieren von CA RCM-Abfragen in CA Enterprise Log Manager

Um CA Enterprise Log Manager-Nutzungsdaten in CA RCM zu importieren, fügen Sie die CA RCM-Datenabfragen der CA Enterprise Log Manager-Abfrageliste hinzu.

So importieren Sie CA RCM-Abfragedateien in CA Enterprise Log Manager

1. Melden Sie sich als Administrator bei CA Enterprise Log Manager an.
2. Navigieren Sie zu "Abfragen und Berichte", "Abfragen".

3. Klicken Sie unter "Abfrageliste" auf "Optionen", "Abfragedefinitition importieren".
4. Geben Sie die Datei "RCM_Queries.xml" an, die sich in dem folgenden Verzeichnis auf dem CA RCM-Server befindet:

   RCM_install\Server\ELM

   Hinweis: *RCM_install* ist das CA RCM-Installationsverzeichnis.

   CA Enterprise Log Manager importiert die Abfragen.

CA RCM führt diese Abfragen aus, um CA Enterprise Log Manager-Abfrageergebnisse anzuzeigen, wenn Benutzer auf überwachte Ressourcen klicken.

Erstellen eines CA Enterprise Log Manager-Sicherheitszertifikats

Um CA RCM zu erlauben, mit CA Enterprise Log Manager zu kommunizieren, erstellen Sie ein CA Enterprise Log Manager-Sicherheitszertifikat und aktualisieren Sie den Schlüsselspeicher mit dem neuen Zertifikat.

Hinweis: Die folgenden Schritte sind speziell für Internet Explorer 8. Falls Sie einen anderen Browser verwenden, lesen Sie in der Dokumentation des Browsers, wie ein Sicherheitszertifikat erstellt wird.

Erstellen Sie ein CA Enterprise Log Manager-Sicherheitszertifikat im Schlüsselspeicher des CA RCM-Servers.

1. Verwenden Sie vom CA RCM-Server aus Internet Explorer, um sich am CA Enterprise Log Manager-API-Portal anzumelden. Verwenden Sie die folgende URL, um auf das API-Portal zuzugreifen:

   https://*calm_hostname:port*/spin/calmapi/calmapi.csp

   Ein Sicherheitszertifikatfehler wird angezeigt.
2. Klicken Sie auf "Laden dieser Website fortsetzen".

   Eine Zertifikatfehlerschaltfläche wird rechts von der Adressleiste des Browsers angezeigt.
3. Klicken Sie auf "Zertifikatfehler", "Zertifikate anzeigen".

   Das Dialogfeld "Zertifikat" zeigt Informationen zum CA Enterprise Log Manager-Sicherheitszertifikat.
4. Klicken Sie auf die Registerkarte "Details" und anschließend auf "In Datei kopieren".

   Der Assistent zum Zertifikatimport wird angezeigt:

5. Exportieren Sie das Zertifikat mithilfe des Assistenten folgendermaßen:
   a. Im Fenster "Exportformat" wählen Sie "Base-64 encoded X.509 (.CER)".
   b. Legen Sie den Dateinamen für das Zertifikat auf "elm_cer.cer" fest.
   c. Klicken Sie auf "Fertig stellen".

   Das Zertifikat wird auf dem CA RCM-Server gespeichert.

6. Aktualisieren Sie den Schlüsselspeicher mit dem Zertifikat folgendermaßen:
   a. Öffnen Sie auf eine Eingabeaufforderung auf dem CA RCM-Server.
   b. Navigieren Sie zu dem Verzeichnis, das das exportierte Zertifikat enthält.
   c. Geben Sie folgenden Befehl ein:

      ```
      "%JAVA_HOME%\bin\keytool.exe" -import -file "Pfadname_Zert"-keystore
      "%JAVA_HOME%\jre\lib\security\cacerts" -trustcacerts
      ```

      Hinweis: Pfadname_Zert ist der Pfadname des exportierten Zertifikats.

      Sie werden aufgefordert, ein Kennwort einzugeben.

   d. Geben Sie das folgende Kennwort oder das Standard-cacerts-Kennwort für Ihr System ein:

      "changeit"

   e. Bei der Frage "Diesem Zertifikat vertrauen?" geben Sie J (Y) ein, und drücken Sie anschließend die Eingabetaste.

   Das CA Enterprise Log Manager-Zertifikat wird im Schlüsselspeicher installiert.

7. Vergewissern Sie sich, dass das neue Zertifikat folgendermaßen angezeigt wird:
   a. Geben Sie folgenden Befehl ein:

      ```
      “%JAVA_HOME%\bin\keytool.exe” -list –keystore
      "%JAVA_HOME%\jre\lib\security\cacerts"
      ```

   b. Geben Sie das cacerts-Kennwort ein.

      Eine Liste von Zertifikaten wird angezeigt.

   c. Stellen Sie sicher, dass ein neues Zertifikat in der Liste angezeigt wird.

8. Starten Sie den Anwendungsserver, auf dem CA RCM gehostet wird.

Registrieren von CA RCM auf dem CA Enterprise Log Manager-Server

Damit CA Enterprise Log Manager den CA RCM-Server erkennen kann, muss CA RCM mit dem CA Enterprise Log Manager-Server registriert werden.

So registrieren Sie CA RCM auf dem CA Enterprise Log Manager-Server

1. Melden Sie sich über folgende URL-Adresse als *EiamAdmin*-Administrator beim CA Enterprise Log Manager-Server an:

   https://*ELM_host*:5250/spin/calmapi/products.csp

   Hinweis: *"ELM_host"* ist der Hostname des CA Enterprise Log Manager-Servers.

2. Klicken Sie unter "Registrierte Produkte" auf "Registrieren".

   Das Fenster "Neue Produktregistrierung" wird angezeigt.

3. Geben Sie den Namen und das Kennwort ein, das Sie für das CA Enterprise Log Manager-Sicherheitszertifikat angegeben haben, und klicken Sie anschließend auf "Registrieren".

   Der CA Enterprise Log Manager-Server erkennt das Zertifikat und genehmigt Verbindungen zu CA RCM.

Aktualisierung von CA RCM-Eigenschaften

Damit der CA RCM-Server mit CA Enterprise Log Manager kommunizieren kann, müssen Sie die CA RCM-Systemeigenschaften aktualisieren.

So aktualisieren sie die CA RCM-Eigenschaften

1. Gehen Sie im CA RCM-Portal zu "Verwaltung", "Einstellungen", "Eigenschaftseinstellungen".
2. Stellen Sie den Filter "Eigenschaftsschlüssel" auf Schlüssel ein, die "logmanager" enthalten.
3. Klicken Sie auf "Filter anwenden".

4. Bearbeiten Sie die folgenden CA RCM-Systemeigenschaften:

   usage.import.logmanager.odbc.host

   Definiert den Hostnamen des Ziel-CA Enterprise Log Manager-Servers.

   usage.import.logmanager.odbc.port

   Definiert den Standard-CA Enterprise Log Manager-Datenbankport.

   Standard: 17002

   Hinweis: Um den Datenbankport zu überprüfen, den CA Enterprise Log Manager überwacht, öffnen Sie die "Verwaltung" in Windows und wählen Sie "Dienste", "ODBC-Server". Klicken Sie auf den CA Enterprise Log Manager-Server und überprüfen Sie das Feld "Überwachungsport für Server".

   usage.import.logmanager.odbc.user

   Definiert den Benutzernamen des CA Enterprise Log Manager-Kontos, das CA RCM verwendet, um sich bei CA Enterprise Log Manager anzumelden. Dies muss ein Administratorkonto in CA Enterprise Log Manager oder ein Konto sein, das Lesezugriff zu allem hat.

   usage.import.logmanager.odbc.password

   Definiert das Kennwort des CA Enterprise Log Manager-Kontos, das CA RCM verwendet, um sich bei CA Enterprise Log Manager anzumelden.

   usage.online.logmanager.https.port

   Definiert den Hostnamen des Ziel-CA Enterprise Log Manager-Servers.

   usage.online.logmanager.https.port

   Definiert den Überwachungsort auf dem Ziel-CA Enterprise Log Manager-Server-Portal.

   Standard: 5250

   usage.online.logmanager.https.certificate

   Gibt den CA Enterprise Log Manager-Sicherheitszertifikatsnamen an, der festgelegt wurde, als CA RCM auf dem CA Enterprise Log Manager-Server registriert wurde.

5. Gehen Sie zum Fenster "Eigenschaftseinstellungen" zurück und legen Sie den Filter "Eigenschaftsschlüssel" für Schlüssel fest, die "accounts" enthalten.

6. Klicken Sie auf "Filter anwenden".
7. Überprüfen Sie die folgenden CA RCM-Eigenschaften. Üblicherweise werden die Standardwerte dieser Eigenschaften nicht geändert, aber es nützlich, etwas über diese Eigenschaften zu wissen:

   implicit.accounts.field.name

   Definiert das CA RCM-Attribut, das verwendet wird, um CA Enterprise Log Manager-Konto-IDs abzugleichen. Wenn Sie ein anderes CA RCM-Attribut, wie PMF-Key oder UUID abgleichen möchten, geben Sie dieses Attribut in dieser Eigenschaft an.

   implicit.accounts.enabled

   Gibt an, ob automatischer impliziter Abgleich von Konten zwischen CA RCM und CA Enterprise Log Manager geschieht.

   Standard: True (Wahr)

Festlegen des Anwendungsattributs im Universum

Um Anwendungen zwischen CA RCM und CA Enterprise Log Manager zuzuordnen, geben Sie zuerst an, welches ResName-Attribut (siehe Seite 316) innerhalb des CA RCM-Universums sich mit einer Anwendung verbindet. ResName2 ist oft das richtige Attribut, aber dieses Attribut hängt davon ab, wie Daten in CA RCM importiert wurden.

Um dieses Attribut im Universum zu definieren, gehen Sie auf "Verwaltung", "Einstellungen", "Einstellungen des Universums", und bearbeiten das Universum. Wählen Sie unter dem Feld der Ressourcen-Anwendung der Konfiguration das Attribut aus, das die Anwendung definiert.

Zuordnen von CA Enterprise Log Manager-Endpunkten

Sie müssen CA Enterprise Log Manager-Anwendungen den CA RCM-Ressourcen zuordnen. Eine Ereignisquelle oder Anwendung in CA Enterprise Log Manager kann einer individuellen Ressource in CA RCM entsprechen.

Ordnen Sie jeder Ressource im CA RCM-Zieluniversum Anwendungen aus CA Enterprise Log Manager zu. CA Enterprise Log Manager-Nutzungsdaten sind dann ordnungsgemäß mit CA RCM-Ressourcen verbunden.

So ordnen Sie CA RCM CA Enterprise Log Manager-Anwendungen zu

1. Gehen Sie im CA RCM-Portal auf "Verwaltung", "Einstellungen","Einstellungen des Universums".

   Das Fenster "Einstellungen des Universums" wird geöffnet.

2. Wählen Sie das Zieluniversum aus und klicken Sie auf "Bearbeiten".

   Das Fenster "Bearbeiten" wird angezeigt:

3. Wählen Sie unter der Registerkarte "Tatsächliche Nutzung", "Einstellungen" das Kontrollkästchen "Importieren Sie und zeigen Sie Nutzungsdaten für dieses Universum an" aus.

4. Klicken Sie auf "Nutzungsdaten jetzt aktualisieren".

   Hinweis: Sie müssen zuerst Daten von CA Enterprise Log Manager importieren, um eine Liste aller Anwendungen zu erhalten, bevor Sie die Anwendungen den CA RCM-Ressourcen zuordnen.

5. Klicken Sie auf die Registerkarte "Anwendungszuordnung".

6. Ordnen Sie CA RCM CA Enterprise Log Manager-Anwendungen folgendermaßen zu:

   a. Der linke Fensterbereich enthält eine Liste aller Anwendungen im CA RCM-Universum. Wählen Sie eine CA RCM-Anwendung aus.

   b. Der rechte Fensterbereich enthält eine Liste aller Anwendungen in CA Enterprise Log Manager. Wählen Sie die CA Enterprise Log Manager-Anwendung aus, die sie der ausgewählten CA RCM-Anwendung zuordnen wollen.

   c. Klicken Sie auf "Hinzufügen".

      Zugeordnete Anwendungen werden im mittleren Bereich angezeigt.

   d. Wiederholen Sie diese Schritte für alle Anwendungen.

7. Klicken Sie auf "Fertig stellen", um die Einstellungen zu speichern.

Aktualisieren von Nutzungsdaten

Wenn Sie CA Enterprise Log Manager-Nutzungsdaten für ein Universum importieren, werden die Nutzungsdaten in allen Zertifizierungs- und Genehmigungsfenstern für dieses Universum angezeigt. Nutzungsdaten werden auch angezeigt, wenn Sie eine Konfiguration des Universums im Entitäten-Browser anzeigen.

So aktualisieren Sie Nutzungsdaten

1. Gehen Sie im CA RCM-Portal auf "Verwaltung", "Einstellungen","Einstellungen des Universums".

   Das Fenster "Einstellungen des Universums" wird geöffnet.

2. Klicken Sie bei dem Universum, das Sie bearbeiten möchten, auf "Bearbeiten".

   Das Fenster "Universum bearbeiten" wird angezeigt.

3. Klicken Sie auf die Registerkarte "Tatsächliche Nutzung".

4. Um CA Enterprise Log Manager-Nutzungsdaten zu aktualisieren, wählen Sie "Importieren" aus und zeigen Sie die Nutzungsdaten für dieses Universum an.

5. (Optional) Geben Sie Nutzungsgrenzwerte an, die das in Zertifizierungs- und Entitätsfenstern angezeigte Symbol bestimmen.

   Im Hinblick auf diesen Grenzwert werden Ressourcen als "Häufig verwendet" oder "Selten verwendet" gekennzeichnet und Benutzer als "Häufige Benutzer" oder "Gelegentliche Benutzer".

6. (Optional) Bearbeiten Sie die Einstellungen des Standardzeitraums. Wenn Sie den Fensterbereich "Zeitraum" erweitern, können Sie die Standardeinstellungen für kurze, mittlere und lange Zeiträume bearbeiten. Das Bearbeiten dieser Werte verändert die verfügbaren Werte in der Drop-down-Liste des Fensterbereichs "Grenzwerte".

7. Klicken Sie auf "Speichern".

8. Klicken Sie auf "Nutzungsdaten jetzt aktualisieren".

Anzeigen der Nutzungsdaten eines Benutzers während einer Kampagne

Nachdem Sie die Integration mit CA Enterprise Log Manager konfiguriert haben, können Kampagnenprüfer die Nutzungsinformationen eines Benutzers anzeigen, bevor sie eine Benutzeraufgabe in ihrem Posteingang genehmigen oder ablehnen.

So zeigen Sie während einer Kampagne Nutzungsdaten eines Benutzers an

1. Gehen Sie auf "Posteingang", "Meine Aufgaben".
2. Klicken Sie unter "Benutzeraufgaben" auf den Link für den Benutzer, dessen Nutzungsdaten Sie überprüfen wollen.

   Ein neues Fenster mit den Benutzerinformationen öffnet sich.
3. Klicken Sie auf die Registerkarte.

   Das Fenster "Ressourcennutzung" wird angezeigt.
4. In der Drop-down-Liste "Anzeigen" wählen Sie "Nutzungsansicht" aus.

   Für diesen Benutzer werden die Nutzungsinformationen pro Anwendung angezeigt.

Aktualisieren der Zuordnung von CA Enterprise Log Manager-Anwendungen

Im Laufe der Zeit werden neue Anwendungen zu CA Enterprise Log Manager hinzugefügt. Es werden auch neue Ressourcen zur CA RCM-Konfiguration hinzugefügt, die neue externe Anwendungen darstellen. Aktualisieren Sie die Anwendungszuordnung im Universum in regelmäßigen Zeitabständen, damit Benutzerinformationen für diese neuen Ressourcen importiert werden.

Verwenden Sie die standardmäßige Prozedur, um neue CA Enterprise Log Manager-Anwendungen zuzuordnen (siehe Seite 247).

Helpdesk-Integration

CA RCM kann so konfiguriert werden, dass es mit anderen Helpdesk-Systemen, wie CA Service Desk Manager, integriert werden kann. In dieser Version ist die Helpdesk-Integration auf die Anzeige von Informationen im CA RCM-Ticket beschränkt. Sobald Sie die Integration konfiguriert haben, können Sie diese Informationen in einem Helpdesk-Ticket anzeigen.

Hinweis: Keinen benutzerdefinierten CA RCM-Eigenschaften oder Vorgänge werden derzeit für diese Integration zur Verfügung gestellt.

Um die Helpdesk-Integration für CA RCM zu konfigurieren, führen Sie den folgenden Prozess aus.

1. Legen Sie Eigenschaften für die Helpdesk-Integration in CA RCM fest.
2. Importieren Sie Helpdesk-Benutzerinformationen in CA RCM.

Festlegen von Eigenschaften für die Helpdesk-Integration

Um die Helpdesk-Integration einzurichten, legen Sie grundlegende sowie Tickettyp-Zuordnungseigenschaften im CA RCM-Portal fest.

So legen Sie Eigenschaften für die Helpdesk-Integration fest

1. Gehen Sie im CA RCM-Portal auf "Verwaltung", "Einstellungen", "Eigenschaftseinstellungen".

   Das Fenster "Eigenschaften" wird angezeigt:

2. Klicken Sie auf "Neu hinzufügen" (oder "Bearbeiten", wenn die Eigenschaft bereits existiert) und legen Sie die folgenden Eigenschaften fest:

   tmsEvent.create.enable

   Definiert, ob Ereignisse der CA RCM-Ticketerstellung, wie eine Helpdesk-Anwendung, an Kunden delegiert werden sollen.

   Werte: True/False (Wahr/Falsch)

   integration.unicenter.servicedesk.username

   Definiert den Helpdesk-Benutzernamen für den Zugriff auf CA RCM, zum Beispiel Administrator.

   integration.unicenter.servicedesk.password

   Definiert das Kennwort für den Helpdesk-Benutzer.

integration.unicenter.servicedesk.webservice.url

Definiert die Helpdesk-Webservice-URL.

Hinweis: CA Help Desk r12 enthält einen neuen Webservice, CA RCM unterstützt jedoch nur den r11-Webservice.

integration.unicenter.servicedesk.user.field

Definiert das Feld in der Benutzerdatenbank zur Berechtigungskonfiguration (eurekify.udb), das die Anmelde-ID des Benutzers im Helpdesk-System angibt.

Hinweis: Wenn keine Angabe gemacht wird, wird die Personen-ID verwendet.

integration.unicenter.servicedesk.type.mapping

Definiert die Zuordnung zwischen RCM-Tickettypen und den Helpdesk-Tickettypen über ein Schlüsselwertepaar.

Beispiel: TMS:TestTicket=*ChangeOrder*,SAGE:*RoleTicket=Bug, SAGE:ErrTicket=Issue

Das aufgeführte Beispiel beschreibt Folgendes:

- Das CA RCM-Testticket wird dem Helpdesk *ChangeOrder* zugeordnet.
- Das CA RCM-Fehlerticket wird dem Helpdesk "Issue" zugeordnet.
- Alle CA RCM-Tickets mit einem Typ, der in "RoleTicket" endet werden einem Helpdesk-Ticket des Typs "Bug" zugeordnet. (SAGE:*RoleTicket=Bug)

integration.unicenter.servicedesk.object.type.*ChangeOrder*

Definiert den Helpdesk-Objekttyp des Tickets *ChangeOrder.*

integration.unicenter.servicedesk.attributes.*ChangeOrder*

Definiert Attribute des Tickets *ChangeOrder*. Verwenden Sie die Velocity Template Language, um Werte für diese Eigenschaft festzulegen. Vordefinierte Variablen (siehe Seite 252) sind verfügbar, um diese Werte festzulegen.

Beispiele:

```
chg_ref_num, RCM_1_${ticket.getTicketId()}_${currentTime},
description, ${ticket.getDescription()},
summary, ${ticket.getTitle()},
affected_contact, ${ticketOwnerHandle},
requestor, ${loginUserHandle} =
```

Hinweis: Weitere Informationen zur Velocity Template Language finden Sie unter http://velocity.apache.org/engine/releases/velocity-1.6.2/user-guide.html.

Vordefinierte Variablen

Die folgenden Variablen können verwendet werden, um Helpdesk-Ticketattribute anzugeben. Diese Variablen werden beim Festlegen der Eigenschaft "integration.unicenter.servicedesk.attributes.*ChangeOrder*" verwendet.

- sid – Ergebnis der Methode "service.login()"
- ticket – TicketVO-Instanz Weitere Informationen finden Sie in der Dokumentation zu TicketVO-Klassen in der offenen API.
- service – Webservice-Instanz, generiert über http://some_server:8080/axis/services/USD_WebServiceSoap?wsdl
- ticketOwnerHandle – Von der Methode "service.getHandleForUserid()" zurückgegebene Bearbeitung des Benutzers, auf den sich das Ticket bezieht
- loginUserHandle – Von der Methode "service.getHandleForUserid()" zurückgegebene Bearbeitung des Benutzers, der unter "integration.unicenter.servicedesk.username" angegeben wurde
- currentTime – System.currentTimeMillis();
- currentDateObject – "java.util.Date"-Darstellung von "System.currentTimeMillis"
- currentTimeFormatted – SimpleDateFormat.getTimeInstance().format(currentDateObject)

- currentDateFormatted – SimpleDateFormat.getDateInstance().format(currentDateObject)
- ticketLinkHtml – Html-Linkelement (Aktion:) mit einer Referenz zum CA RCM-Ticket
- ticketQueueUrl – Wert der Eigenschaft "portalExternalLink.ticketQueueUrl" Zum Beispiel, http://localhost:8080/eurekify/

Importieren von Helpdesk-Benutzerinformationen in "eurekify.udb"

Um die Helpdesk-Integration abzuschließen, legen Sie die Berechtigungskonfiguration des Helpdeskbenutzers in der CA RCM-Benutzerdatenbank (eurekify.udb) fest.

So importieren Sie Helpdesk-Benutzerinformationen

1. Gehen Sie in CA RCM Data Management auf "Datei" und "Von Datenbank öffnen".

   Das Fenster "Datenverwaltungseinstellungen" wird angezeigt.
2. Wählen Sie "Benutzerdatenbankdateien" in der Dropdown-Liste "Dateityp auswählen".
3. Wählen Sie "Eurekify_Users.udb" aus und klicken Sie auf "Weiter".
4. Gehen Sie auf "Datei", "Datei speichern als" und speichern Sie "Eurekify_Users.udb" als eine Datei.
5. Bearbeiten Sie die gespeicherte Datei und fügen Sie die Informationen zu Helpdesk-Kontonamen als zusätzliches Feld hinzu.
6. Gehen Sie in CA RCM Data Management auf "Verwaltung", "Benutzerdatenbank zusammenführen", und führen Sie die gespeicherte Datei mit der Datenbank folgendermaßen zusammen:
   a. Geben Sie im Feld "Dateien" die folgenden Werte ein:
      - Erste Benutzerdatenbank: Pfad zur gespeicherten Datenbankdatei, die Sie in Schritt 5 bearbeitet haben
      - Zweite Benutzerdatenbank: Pfad zur ursprünglichen CA RCM-Datenbank
      - Ausgabe-Benutzerdatenbank: Pfad zur CA RCM-Ausgabedatenbank
   b. Klicken Sie auf "Zusammenführen".

Das Transaktionsprotokoll

Das CA RCM-Transaktionsprotokoll (TxLog) enthält detaillierte Informationen über die auf dem CA RCM-Server ausgeführten Aktionen. Das Transaktionsprotokoll zeichnet auch alle Änderungen an Benutzer-, Rollen- und Ressourcenentitäten auf.

Hinweis: Das Transaktionsprotokoll zeichnet Entitätsänderungen nur für die von Ihnen angegebenen Datendateien auf. Weitere Informationen finden Sie im *Datenmanagement-Benutzerhandbuch* oder im *DNA-Benutzerhandbuch*.

Eine Übersicht über die Transaktionsprotokolleinträge finden Sie im Ordner "Developer Resource" der Datei **CA-RCM-rel#-Language-Files.zip** des CA RCM-Installationspakets.

Wenn Sie die Seite "Transaktionsprotokoll" zum ersten Mal öffnen, ist die Tabelle leer und es wird ein Filter angezeigt, den Sie verwenden können, um die Transaktionen auszuwählen, die Sie anzeigen möchten. Die Einträge sind nach Datum geordnet aufgelistet.

<Spalte>

Wählen Sie die Spalte aus, die festlegt, welche Transaktionen in der Transaktionsprotokoll-Tabelle angezeigt werden. Die Kriterien zur Filterung des Tabelleninhalts basieren auf folgenden Optionen:

- Quelle: Das Subsystem, aus dem die Transaktion hervorgegangen ist.
- Besitzer: Besitzer oder Ticket-ID
- SData1
- SData2
- SData3

<Textbox>

Geben Sie beliebige Daten ein, die in der ausgewählten Spalte erscheinen können, um die Transaktionen weiter zu filtern. Beim Text wird Groß- und Kleinschreibung beachtet

OK

Aktualisiert die in der Transaktionsprotokoll-Tabelle angezeigten Daten. Wenn kein Filter angewendet wurde, werden alle bestehenden Transaktionen aufgelistet.

Alle löschen

Löscht alle vom CA RCM-System gespeicherten Transaktionen.

Datensätze pro Seite

Wählen Sie die Anzahl an Datensätzen, die in der Tabelle angezeigt werden.

So zeigen Sie Transaktionen in der Transaktionsprotokoll-Tabelle an.

1. Gehen Sie im CA RCM-Portal zu "Verwaltung" und danach auf "Transaktionsprotokoll".

   Das Fenster "Transaktionsprotokoll" wird angezeigt.

2. (Optional) Filtern Sie die Daten, die Sie anzeigen möchten, in der Transaktionsprotokoll-Tabelle: Wählen Sie ein Feld aus der Dropdown-Box "Spalte" aus und geben Sie den Inhalt des Feldes ein

3. Klicken Sie auf "OK".

   Die angeforderten Transaktionsprotokolle werden in der Transaktionsprotokoll-Tabelle angezeigt.

4. (Optional) Klicken Sie auf "Alle löschen", um alle Transaktionen, die derzeit vom System gespeichert werden, zu löschen.

Überwachen der Portalnutzung mithilfe des Transaktionsprotokolls

Der CA RCM-Server verzeichnet Benutzeraktioinen und Änderungen an Entitäten in der Transaktionsprotokolldatei. Sie können die Benutzerinteraktion mit dem CA RCM-Portal im Transaktionsprotokoll überwachen.

Hinweis: Sie benötigen Administrator-Berechtigungen im CA RCM-Portal, um diesen Vorgang auszuführen.

So überwachen Sie die Portalnutzung mithilfe des Transaktionsprotokolls

1. Gehen Sie im CA RCM-Portal zu "Verwaltung", "Einstellungen", "Eigenschaftseinstellungen".

   Das Fenster "Eigenschaftseinstellungen" wird angezeigt.

2. Ändern Sie die folgenden Systemeigenschaften von CA RCM, um die Überwachung der Portalnutzung zu konfigurieren und zu aktivieren.

   Hinweis: Um alle Systemeigenschaften anzuzeigen, die sich auf die Überwachung im Transaktionsprotokoll auswirken, filtern Sie in der Eigenschaftenliste mithilfe der Zeichenfolge "**txlog"**.

   txlog.portal.login.enable

   Gibt an, ob ein Ereignis im Transaktionsprotokoll festgehalten werden soll, wenn sich ein Benutzer beim CA RCM-Portal anmeldet.

   Werte: Wahr, Falsch

   txlog.portal.logout.enable

   Gibt an, ob ein Ereignis im Transaktionsprotokoll festgehalten werden soll, wenn sich ein Benutzer beim CA RCM-Portal abmeldet.

   Werte: Wahr, Falsch

   txlog.webservice.login.enable

   Gibt an, ob ein Ereignis im Transaktionsprotokoll festgehalten werden soll, wenn sich ein Webservice beim CA RCM-Portal anmeldet.

   Werte: Wahr, Falsch

   txlog.portal.pageaccess.enable

   Gibt an, ob Ereignisse im Transaktionsprotokoll festgehalten werden sollen, wenn Benutzer im CA RCM-Portal navigieren.

   Werte: Wahr, Falsch

txlog.portal.pageaccess.include.pageclasses

Gibt die Portalseiten an, die einbezogen werden sollen, wenn die Benutzernavigation im CA RCM-Portal überwacht wird. Portalseiten nach ihren Klassennamen identifizieren und die Werte als Liste mit kommagetrennten Werten (CSV) ausgeben

Beispiel: Die folgende Zeichenfolge erlaubt die Überwachung der Benutzernavigation zur Hauptseite des Portals sowie zum Dashboard und den Seiten des Entitäten-Browsers auf oberster Ebene:

```
com.eurekify.web.portal.homepage.HomePage,com.eurekify.web.dashboards.Con
figurationDashboardPage,com.eurekify.web.entitybrowser.EurekifyBrowserPag
e
```

txlog.portal.pageaccess.include.pageclasses

Gibt die Portalseiten an, die ausgeschlossen werden sollen, wenn die Benutzernavigation im CA RCM-Portal überwacht wird. Portalseiten nach ihren Klassennamen identifizieren und die Werte als Liste mit kommagetrennten Werten (CSV) ausgeben

Standard: com.eurekify.web.portal.EmptyPage

3. Speichern Sie die Änderungen in den Systemeigenschaften.

   Interaktionen mit dem CA RCM-Portal werden wie festgelegt im Transaktionsprotokoll aufgezeichnet.

Weitere Informationen:

So bearbeiten Sie einen Eigenschaftsschlüssel (siehe Seite 271)

Cache-Bearbeitung

Die Verwendung des Cache des CA RCM-Servers verbessert die Leistung. Dies wird durch das Hochladen des aktuellen Universums und der aktuellen Konfigurationsdaten in den Cache erreicht. Der Zugriff auf den Cache des Servers ist wesentlich schneller als der Zugriff auf Festplatten, so können Benutzer Informationen schneller erhalten, als wenn Sie Inhalte von den Festplatten des Servers erhalten müssen.

Dieser Abschnitt umfasst folgende Themen:

- Laden des Zwischenspeichers
- Zwischenspeicher leeren

Weitere Informationen:

Laden des Zwischenspeichers (siehe Seite 258)
Leeren des Zwischenspeichers (siehe Seite 259)

Laden des Zwischenspeichers

Dieses Hilfsprogramm wird verwendet, um eine spezifische Konfiguration schnell in den Zwischenspeicher des CA RCM-Servers zu laden.

So laden Sie eine spezifische Konfiguration in den Zwischenspeicher des CA RCM-Servers.

1. Klicken Sie im Menü "Verwaltung" auf "Zwischenspeicher" und wählen Sie anschließend "Zwischenspeicher laden".

   Das Fenster "Zwischenspeicher laden" wird angezeigt.

2. Wählen Sie eine Konfiguration aus der Dropdown-Liste, und klicken Sie auf "OK".

   Die Informationsleiste zeigt an, dass die ausgewählte Konfiguration geladen wird.

Leeren des Zwischenspeichers

Verwenden Sie dieses Hilfsprogramm, um den Zwischenspeicher des CA RCM-Servers zu löschen. Das Hilfsprogramm ist nützlich in dem Fall, dass Sie die Konfigurationsdaten in DNA, wie z. B. Berechtigungen, aktualisiert haben und sicher gehen wollen, dass jemand, der das System verwendet, die aktualisierten Daten verwendet.

So leeren Sie den Zwischenspeicher

1. Klicken Sie im Menü "Verwaltung" auf "Zwischenspeicher leeren".

   Das Fenster "Zwischenspeicher leeren" wird angezeigt.

2. Klicken Sie auf "Zwischenspeicher leeren", um den Zwischenspeicher des CA RCM-Servers zu leeren.

   Die Informationsleiste zeigt an, dass die ausgewählte Konfiguration geladen wird.

Reparieren von CA RCM-Konfigurations-, Benutzer- und Ressourcendateien

Das Bearbeiten und Anreichern von Daten kann in vereinzelten Fällen zu inkonsistenten Benutzer-, Ressource- oder Konfigurationsdateien führen. Sie können Konfigurationen und die in Verbindung stehenden Benutzer- und Ressourcendatendateien analysieren, und eventuelle Inkonsistenzen beheben. Wenn Sie Benutzer- (.udb), Ressourcen- (.rdb) oder Konfigurationsdateien (.cfg) nicht öffnen können, überprüfen Sie sie mit Hilfe dieses Vorgangs auf Fehler.

Hinweis: Sie benötigen Administrator-Berechtigungen im CA RCM-Portal, um diesen Vorgang auszuführen.

So reparieren Sie CA RCM-Konfigurations-, Benutzer- und Ressourcendateien

1. Gehen Sie im CA RCM-Portal zu "Verwaltung", dann auf "Einstellungen", anschließend auf "Konfiguration reparieren".

   Das Fenster "Konfiguration reparieren" wird angezeigt.

2. Wählen Sie eine Konfigurationsdatei aus der Dropdown-Liste, und klicken Sie auf "Analysieren".

   CA RCM analysiert die Konfigurationsdatei und die entsprechenden Benutzer- und Ressourcendateien. Folgende Fehler können entdeckt werden:

   - Verwaiste Benutzer oder Ressourcen – Die Konfigurationsdatei listet Benutzer bzw. Ressourcen auf, die nicht in der Quellbenutzer- (.udb) oder Ressourcendatei (.rdb) vorhanden sind.
   - Fehlerhafte Links – Ein Link bezieht sich auf Benutzer, Ressourcen oder Rollen, die in der Konfiguration nicht mehr vorhanden sind.
   - Nicht sequenzielle Benutzer- oder Ressourcendatei – Jedem Datensatz in Benutzer- oder Ressourcendateien wird eine interne ID zugewiesen. Wenn es sich dabei nicht um aufeinanderfolgende IDs handelt, kann CA RCM die Datei nicht öffnen.

3. Führen Sie einen der folgenden Schritte aus:

   - Wenn die Analyse verwaiste Benutzer oder Ressourcen bzw. fehlerhafte Links in der Konfiguration findet, klicken Sie auf "Konfiguration reparieren".

     Verwaiste Entitäten und die entsprechenden Links werden entfernt. Fehlerhafte Links werden auch entfernt.

   - Wenn die Analyse eine nicht sequenzielle Benutzerdatei findet, klicken Sie auf "Benutzerdatenbank reparieren".

     Die Benutzerdatei (.udb) erhält eine neue Nummerierung. Zusätzlich werden in *allen* Konfigurationen, die auf diese Benutzerdatei verweisen, die verwaisten Benutzer und fehlerhaften Benutzerlinks gelöscht. Anschließend werden die Benutzerlisten und die Benutzerlinks dieser Konfigurationen mit den neuen IDs aktualisiert.

     Hinweis: Diese Funktion betrifft neben der von Ihnen analysierten Konfiguration weitere Konfigurationen. Überprüfen Sie vor der Ausführung dieser Funktion in Verbindung stehende Konfigurationen sowie deren Inhalt.

- Wenn die Analyse eine nicht sequenzielle Ressourcendatei findet, klicken Sie auf "Ressourcendatenbank reparieren".

  Die Ressourcendatei (.rdb) erhält eine neue Nummerierung. Zusätzlich werden in *allen* Konfigurationen, die auf diese Ressourcendatei verweisen, die verwaisten Ressourcen und fehlerhaften Ressourcenlinks gelöscht. Anschließend werden die Ressourcenlisten und die Ressourcenlinks dieser Konfigurationen mit den neuen IDs aktualisiert.

  Hinweis: Diese Funktion betrifft neben der von Ihnen analysierten Konfiguration weitere Konfigurationen. Überprüfen Sie vor der Ausführung dieser Funktion in Verbindung stehende Konfigurationen sowie deren Inhalt.

Löschen von Daten

Ein gutes Management erfordert die regelmäßige Löschung alter, nicht mehr gebrauchter Datendateien vom CA RCM-Datenbankserver. Das Lösch-Hilfsprogramm vereinfacht diese Wartungsaufgabe.

Wichtig! Ein Löschvorgang entfernt Daten vollständig und anhaltend aus CA RCM-Datenbanken. Sichern Sie alle Daten, bevor Sie sie löschen, und stellen Sie sicher, dass die Daten, die Sie löschen, nicht gebraucht werden.

Mit dem Lösch-Hilfsprogramm können Sie Daten auf folgende Weisen entfernen:

- Ausgewählte Dokumente und Datendateien löschen
- Nach Datum löschen - Löschen Sie Einträge, die älter als das von Ihnen angegebene Datum sind, aus der Datenbank oder den Systemprotokollen.
- Inaktive Portal-Benutzer löschen - Entfernen Sie CA RCM-Portalbenutzer, die sich nicht mit mindestens einem Universum assoziiert sind.

Das Lösch-Hilfsprogramm löscht keine Jobs aus der Workpoint-Datenbank. Sie müssen Workpoint-Jobs manuel auswählen und löschen (siehe Seite 266).

Löschen von ausgewählten Dokumenten

Sie können das Lösch-Hilfsprogramm des CA RCM-Portals nutzen, um veraltete oder nicht mehr gebrauchte Datendateien aus der CA RCM-Datenbank zu löschen.

Wichtig! Ein Löschvorgang entfernt Daten vollständig und anhaltend aus CA RCM-Datenbanken. Sichern Sie alle Daten, bevor Sie sie löschen, und stellen Sie sicher, dass die Daten, die Sie löschen, nicht gebraucht werden.

Wenn Sie eine Universums- oder Konfigurationsdatei löschen, werden folgende damit verbundenen Dateien auch gelöscht:

- Verwandte Konfigurationsdateien wie Master-, Modell- und RACI-Konfigurationen.
- Auditkarten
- Kampagnen
- Protokolleinträge

Hinweis: Sie benötigen Administrator-Berechtigungen im CA RCM-Portal, um diesen Vorgang auszuführen.

So löschen Sie ausgewählte Dokumente

1. Gehen Sie im CA RCM-Portal zu "Verwaltung", dann auf "Einstellungen", anschließend auf "Daten löschen".

   Das Fenster "Daten löschen" wird angezeigt.

2. Aktivieren Sie die Option "Nach Dokument" in der Dropdown-Liste "Typ der Löschung", und klicken Sie anschließend auf "Weiter".

3. Wählen Sie den Dokumenttyp, den Sie löschen möchten, aus der Dropdown-Liste "Typ der Löschung" aus.

   Das Fenster "Werte auswählen" wird angezeigt. Alle vorhandenen Datendateien des von Ihnen festgelegten Typs werden aufgelistet.

4. Wählen Sie alle Dokumente aus, die Sie löschen möchten.

   Hinweis: Drücken Sie die Umschalttaste oder nutzen Sie Ihre Maus, um einen Bereich der Liste auszuwählen, oder drücken Sie die Strg-Taste und klicken Sie, um einzelne Dateien aus der Liste auszuwählen.

5. Klicken Sie auf "Next".

   Das Bestätigungsfenster wird angezeigt:

6. Überprüfen Sie den Datenlöschumfang:

   - Erweitern Sie im Bereich Dokumententypen die Struktur, um zu sehen, welche Datendateien zum Löschen ausgewählt sind. Diese Liste schließt Dateien ein, die auf den von Ihnen gewählten Dateien basieren oder sich von ihnen ableiten.
   - Überprüfen Sie im Zählerbereich den Umfang verwandter Protokoll- und Ticketdaten, die zum Löschen ausgewählt sind.

   Wenn der von Ihnen festgelegte Umfang Daten einschließt, die Sie nicht löschen möchten, folgen Sie einer der folgenden Optionen:

   - Klicken Sie auf "Zurück", um die Auswahlkriterien neu festzulegen.
   - Klicken Sie auf "Abbrechen", um den Löschvorgang abzubrechen, und kopieren oder sichern Sie dann die benötigten Daten.

7. Klicken Sie auf "Bereinigen".

   Die festgelegten Daten werden dauerhaft aus der CA RCM-Datenbank gelöscht. Wenn der Löschvorgang abgeschlossen ist, wird eine Bestätigungsmeldung im Fenster "Daten löschen" angezeigt.

Löschen von Daten nach Datum

Sie können das Lösch-Hilfsprogramm verwenden, um Workflow-Tickets, Transaktions-(Tx)-Protokolleinträge oder Portalnutzungsinformationen zu löschen, indem Sie Daten suchen, die älter sind als das von Ihnen festgelegte Datum.

Wichtig! Ein Löschvorgang entfernt Daten vollständig und anhaltend aus CA RCM-Datenbanken. Sichern Sie alle Daten, bevor Sie sie löschen, und stellen Sie sicher, dass die Daten, die Sie löschen, nicht gebraucht werden.

Hinweis: Sie benötigen Administrator-Berechtigungen im CA RCM-Portal, um diesen Vorgang auszuführen.

So löschen Sie Daten nach Datum

1. Klicken Sie im Hauptmenü des CA RCM-Portals auf Verwaltung, Einstellungen, Daten löschen.

   Das Fenster "Daten löschen" wird angezeigt.

2. Aktivieren Sie in der Dropdown-Liste "Löschungstyp" die Option "Nach Datum", und klicken Sie anschließend auf "Weiter".

   Das Fenster "Auswahltyp" wird angezeigt.

3. Wählen Sie den Datentyp, den Sie löschen möchten, aus der Dropdown-Liste "Auswahltyp" aus, und klicken Sie auf "Weiter".

   Das Fenster "Werte auswählen" wird angezeigt.

4. Füllen Sie das folgende Feld aus, um den Löschumfang zu definieren.

   Älter als

   Gibt das Datum des ältesten Eintrags an, der behalten werden soll. Einträge, die vor diesem Datum liegen, werden gelöscht.

5. (Optional nur für Tx-Protokolllöschung) Filtern Sie unter Verwendung der folgenden zusätzlichen Felder Transaktionsprotokolleinträge:

   Eigentümer

   Definiert die Benutzer-ID oder Ticket-ID des initiierenden Benutzers oder Tickets.

   Quelle

   Definiert das CA RCM-Teilsystem, das den Protokolleintrag generiert hat.

   sdata1, sdata2

   Definiert Werte in den Zeichenfolgendatenfeldern der Protokolleinträge.

6. Klicken Sie auf "Next".

   Das Bestätigungsfenster wird angezeigt:

7. Überprüfen Sie den Datenlöschumfang.

8. Klicken Sie auf "Bereinigen".

   Die festgelegten Daten werden dauerhaft und vollkommen aus der CA RCM-Datenbank gelöscht. Wenn der Löschvorgang abgeschlossen ist, wird eine Bestätigungsmeldung im Fenster "Daten löschen" angezeigt.

Löschen von Portalbenutzern aus der Berechtigungskonfiguration

Benutzer verschiedener Ebenen des Unternehmens greifen auf das CA RCM-Portal zu, um an Überprüfungs- und Zertifikationskampagnen teilzunehmen und Self-Service-Rollenmanagement-Tools zu verwenden. Jeder Benutzer muss ein Portalbenutzerkonto haben. CA RCM kann diese Benutzerkonten automatisch, basierend auf den abgerufenen Benutzerdaten erstellen. Die Datei für die *Berechtigungskonfiguration* speichert die Kontoinformationen der Portalbenutzer.

Um die Datenintegrität und Sicherheit des CA RCM-Portals zu bewahren, sollten Sie regelmäßig Benutzer entfernen, die diesen Zugang nicht länger benötigen.

Das Lösch-Hilfsprogramm identifiziert automatisch Portalbenutzer, die nicht mit einem derzeit bestehenden Universum verbunden sind. Diese Benutzer können in keinem der CA RCM-Vorgänge teilnehmen und sind Kandidaten für die nächste Löschung.

Wichtig! Ein Löschvorgang entfernt Daten vollständig und anhaltend aus CA RCM-Datenbanken. Sichern Sie alle Daten, bevor Sie sie löschen, und stellen Sie sicher, dass die Daten, die Sie löschen, nicht gebraucht werden.

Hinweis: Sie benötigen Administrator-Berechtigungen im CA RCM-Portal, um diesen Vorgang auszuführen.

So löschen Sie Portalbenutzer aus der Berechtigungskonfiguration

1. Klicken Sie im Hauptmenü des CA RCM-Portals auf Verwaltung, Einstellungen, Daten löschen.

   Das Fenster "Daten löschen" wird angezeigt.

2. Aktivieren Sie in der Dropdown-Liste "Löschungstyp" die Option "Benutzer der Berechtigungskonfiguration", und klicken Sie anschließend auf "Weiter".

   Der CA RCM-Server vergleicht Portalberechtigungsdaten mit Universumsdateien in der Datenbank. Alle Portalbenutzer, die mit keinem Universum verbunden sind, werden als Löschungskandidaten aufgelistet. Wenn Ihnen Löschungskandidaten angezeigt werden, setzen Sie den Löschvorgang fort.

3. Wählen Sie die Benutzer aus, die Sie löschen möchten, oder klicken Sie auf das Kontrollkästchen am Spaltenkopf, um alle Benutzer auszuwählen.

4. Klicken Sie auf "Next".

   Das Bestätigungsfenster wird angezeigt:

5. Überprüfen Sie den Datenlöschumfang.

   Wenn der von Ihnen festgelegte Umfang Daten einschließt, die Sie nicht löschen möchten, folgen Sie einer der folgenden Optionen:

   - Klicken Sie auf "Zurück", um die Auswahlkriterien neu festzulegen.
   - Klicken Sie auf "Abbrechen", um den Löschvorgang abzubrechen, und kopieren oder sichern Sie dann die benötigten Daten.

6. Klicken Sie auf "Bereinigen".

   Die festgelegten Daten werden dauerhaft aus der CA RCM-Datenbank gelöscht. Wenn der Löschvorgang abgeschlossen ist, wird eine Bestätigungsmeldung im Fenster "Daten löschen" angezeigt.

Workpoint-Jobs löschen, die mit einem Workflow assoziiert sind

CA RCM initiiert Workpoint-Jobs, um Überprüfungs- oder Steueraktionen von Geschäfts-Workflows zu implementieren. So wird zum Beispiel für jeden Link im Rahmen einer Zertifizierungskampagne ein Workpoint-Job erstellt.

Um die Größe der CA RCM-Workpoint-Datenbank zu reduzieren, können Sie die Datensätze von Workpoint-Jobs für Workflows löschen, die abgeschlossen sind.

1. Um Workflows zu identifizieren, die inaktiv sind, filtern Sie im Workflows-Fenster des CA RCM-Portals die Workflows so, dass nur solche angezeigt werden, deren Status "Angehalten", "Archiviert" oder "Abgeschlossen" lautet. Sie können auch nach Fälligkeitsdatum des Workflows filtern. Merken Sie sich die Workflow-ID-Nummern dieser inaktiven Workflows.
2. Durchsuchen Sie auf Ihrem Datenbankserver die CA RCM-Workpoint-Datenbank nach Jobentitäten mit diesen Workflow-ID-Werten. Löschen Sie dann die ausgewählten Jobs.

Beispiel: Job-Bereinigungs-Skript in SQL

Normalerweise implementieren Sie ein Datenbankabfrageskript, um die Datenbank zu durchsuchen und zu bereinigen. Das folgende Beispiel zeigt SQL-Befehle, die Jobs, die mit einem einzelnen Workflow assoziiert sind, auswählen und löschen. Bevor Sie diese Befehle an den Datenbankserver senden, ersetzen Sie den Parameter *flow_id* durch den eigentlichen Workflow-ID-Wert.

```
update WP_PROCI set LU_ID = 'Delete Job'
    where CONVERT(varchar(max), WP_PROCI.PROCI_ID)+':'+WP_PROCI.PROCI_DB in
    (select CONVERT(varchar(max),
    WP_USER_DATA.PROCI_ID)+':'+WP_USER_DATA.PROCI_DB
    from WP_USER_DATA
    where WP_USER_DATA.VAR_NAME = 'flow_id'
    and WP_USER_DATA.VAR_CVALUE like '?');
execute spWP_DELETE_JOBS;
```

Eigenschaftseinstellungen

Das Eigenschaftseinstellungs-Hilfsprogramm gewährt Zugriff auf die Systemeigenschaftdatei "CA RCM.properties", in der Sie neue Eigenschaftsschlüssel erstellen und auf vorhandene Eigenschaftsschlüsselwerte zugreifen und sie bearbeiten.

Zur leichteren Handhabung werden Eigenschaften, die als allgemeine Eigenschaften gelten, wie solche des Typs "properties.headers.commonProperties", separat unter dem Einstellungs-Untermenü als Einstellungen von allgemeinen Eigenschaften aufgelistet. Dieses Hilfsprogramm funktioniert auf die gleiche Weise wie das allgemeine Hilfsprogramm zu Eigenschaftseinstellungen.

Die Tabelle "Eigenschaften" enthält folgende Spalten:

Typ

Zugeordneter Eigenschaftsdateiname

Eigenschaftsschlüssel

Name des Eigenschaftsschlüssels

Eigenschaftswert

Zugeordneter Wert für Eigenschaftsschlüssel

Die Seite "CA RCM-Eigenschaften" stellt folgende Funktionen bereit:

Neue hinzufügen

Zur Erstellung neuer Eigenschaftsschlüssel verwenden.

Bearbeiten

Zur Bearbeitung bestehender Eigenschaftsschlüssel verwenden.

Filter anwenden

Zum Filtern der Eigenschaftsliste verwenden.

Datensätze pro Seite

Die Zahl, die verwendet wird, um Eigenschaften zu bestimmen, die in der Tabelle angezeigt werden.

Beim Erstellen eines Schlüssels oder beim Bearbeiten einer vorhandenen Eigenschaft werden die Daten in der CA RCM-Datenbank gespeichert. Beim Ausführen des CA RCM-Portals überprüft der CA RCM-Server die Datenbankeigenschaftslisten. Wenn sich der Wert eines Eigenschaftsschlüssels der Datenbank von einem in der Datei eurekify.properties aufgeführten Wert unterscheidet, wird das System den in der Datenbank aufgeführten Wert verwenden.

Hinweis: Die Datenbankwerte verändern sich nicht während Systemaktualisierungen.

Das CA RCM-Portal stellt Ihnen die folgenden Datenbanken zur Verfügung, in denen Sie Ihre aktualisierten Schlüsselwerte speichern können:

DB_dynamic_properties

Die Änderung wurde unmittelbar umgesetzt. Sie müssen nicht warten, bis der Server offline ist, um die Eigenschaftswerte zu aktualisieren.

DB_static_properties

Die Änderung tritt in Kraft, wenn der Server neu gestartet wird.

Hinweis: Server schalten sich für regelmäßige Wartung und Backups in den Offline-Modus. Änderungen, die an den als "DB_static_properties" gekennzeichneten Eigenschaftswerten vorgenommen wurden, werden implementiert, wenn der Server wieder online ist.

So greifen Sie auf die Seite "Eigenschaften" zu

1. Klicken Sie im Menü "Verwaltung" auf "Einstellungen".

   Die Liste der verfügbaren Optionen wird angezeigt.

2. Klicken Sie auf "Eigenschaftseinstellungen".

   Das Fenster der Seite "CA RCM-Eigenschaften" öffnet sich.

Weitere Informationen:

Zugriff auf die Seite "Allgemeine Eigenschaftseinstellungen" (siehe Seite 269)
CA RCM-Eigenschaften (siehe Seite 311)

Zugriff auf die Seite "Allgemeine Eigenschaftseinstellungen"

Allgemeine Eigenschaften sind Eigenschaften des Typs "properties.headers.commonProperties".

Für Anweisungen darüber, wie man einen neuen Eigenschaftsschlüssel erstellt oder bearbeitet, lesen Sie:

- "Erstellen eines neuen Eigenschaftsschlüssels"
- "Bearbeiten eines bestehenden Eigenschaftsschlüssels"

So greifen Sie auf die Seite "Allgemeine Eigenschaftseinstellungen" zu

1. Klicken Sie im Menü "Verwaltung" auf "Einstellungen".

   Die Liste der verfügbaren Einstellungsoptionen wird angezeigt.

2. Klicken Sie auf "Allgemeine Eigenschaftseinstellungen".

   Das Fenster "Allgemeine Eigenschaftseinstellungen" wird geöffnet.

Weitere Informationen:

"Erstellen eines Eigenschaftsschlüssels" (siehe Seite 270)
So bearbeiten Sie einen Eigenschaftsschlüssel (siehe Seite 271)

"Erstellen eines Eigenschaftsschlüssels"

Eigenschaftsschlüssel werden definiert und als Teil des standardmäßig von CA RCM installierten CA RCM-Produkts zur Verfügung gestellt. Das Eigenschaftseinstellungs-Hilfsprogramm ermöglicht es Ihnen, der CA RCM-Eigenschaftsdatei neue Eigenschaftsschlüssel hinzuzufügen.

Um einen Eigenschaftsschlüssel zu erstellen, geben Sie den Schlüssel ein, bevor Sie auf "Neu hinzufügen" klicken.

Nachdem Sie den neuen Eigenschaftsschlüsselnamen eingegeben und auf "Erstellen" geklickt haben, öffnet sich das Fenster "Eigenschaft bearbeiten".

Die Funktion "Speichern" ist deaktiviert. Der Grund dafür ist, dass, wenn Sie einen Eigenschaftsschlüssel bearbeiten, diese Änderung aus Sicherheitsgründen nicht direkt unter der Eigenschaftsdatei gespeichert wird. Stattdessen wird der aktualisierte Eigenschaftsschlüsselwert in der CA RCM-Datenbank gespeichert.

Das CA RCM-Portal stellt Ihnen zwei Datenbanken zur Verfügung, in denen Sie Ihre aktualisierten Schlüsselwerte speichern können:

DB_dynamic_properties

Die Änderung wurde unmittelbar umgesetzt. Sie müssen nicht warten, bis der Server offline ist, um die Eigenschaftswerte zu aktualisieren.

DB_static_properties

Die Änderung wird beim nächsten Neustart des Servers umgesetzt.

So erstellen Sie einen Eigenschaftsschlüssel

1. Geben Sie auf der Seite "CA RCM-Eigenschaften" in das Textfeld unter "Allgemeine Eigenschaften" den Namen eines Eigenschaftsschlüssels ein.
2. Klicken Sie auf "Neue hinzufügen".

   Das Fenster "Eigenschaft bearbeiten" öffnet sich.
3. Geben Sie einen Eigenschaftswert in das Textfeld ein.
4. Wählen Sie aus der Dropdown-Liste einen Datenbanktyp aus.
5. Klicken Sie auf "Speichern". Die neue Eigenschaft wird im Fenster "Allgemeine Eigenschaftseinstellungen" angezeigt.

So bearbeiten Sie einen Eigenschaftsschlüssel

Nach Systemänderungen kann es notwendig sein, den Wert eines Eigenschaftsschlüssels zu aktualisieren. So müssen zum Beispiel, wenn Sie den Namen des SMTP-Servers (E-Mail) ändern, der von Ihrem Unternehmen zum Versenden von E-Mails verwendet wird, die entsprechenden Eigenschaftsschlüssel ebenfalls angepasst werden.

Wenn Sie neben einem bestehenden Eigenschaftsschlüssel auf "Bearbeiten" klicken, öffnet sich das Fenster "Eigenschaft bearbeiten":

Wenn Sie eine bestehende Eigenschaft bearbeiten, wird die Quelle der Eigenschaft im Typ "Dropdown" aufgelistet.

"Speichern" wird deaktiviert, weil, wenn Sie einen Eigenschaftsschlüssel bearbeiten, der aktualisierte Eigenschaftsschlüsselwert in der CA RCM-Datenbank gespeichert wird.

Das CA RCM-Portal stellt Ihnen die folgenden Datenbanken zur Verfügung, in denen Sie Ihre aktualisierten Schlüsselwerte speichern können:

DB_dynamic_properties

Die Änderung wurde unmittelbar umgesetzt. Sie müssen nicht warten, bis der Server offline ist, um die Eigenschaftswerte zu aktualisieren.

DB_static_properties

Die Änderung wird beim nächsten Neustart des Servers umgesetzt.

So bearbeiten Sie einen Eigenschaftsschlüssel

1. (Optional) Geben Sie auf der Seite "CA RCM-Eigenschaften" den Namen eines Eigenschaftsschlüssels oder einen Teil davon in das Feld "Filtern von Eigenschaftsschlüsseln mit" ein, und klicken sie auf "Filter anwenden".

   Die Eigenschaftstabelle zeigt nur Schlüssel an, die mit Ihren Filterkriterien übereinstimmen.

2. Klicken Sie neben dem Eigenschaftsschlüssel, den Sie ändern möchten, auf "Bearbeiten".

   Das Fenster "Eigenschaft bearbeiten" öffnet sich.

3. Geben Sie einen Eigenschaftswert in das Textfeld ein.

4. Wählen Sie aus der Dropdown-Liste einen Datenbanktyp aus.
5. Klicken Sie auf "Speichern".

   Die aktualisierte Eigenschaft wird in der Tabelle des Fensters "Eigenschaften" angezeigt.

RACI-Vorgänge

Das RACI-Modell ist ein Tool, das zur Identifizierung von Rollen und Zuständigkeiten beim Organisationsaudit verwendet werden kann, womit der Auditprozess einfacher und problemloser ablaufen kann. In diesem Modell wird beschrieben, wer bei einem Audit oder bei Änderungen im Unternhemen wofür zuständig ist.

RACI steht für:

R = Responsible. Der Besitzer des Problems/Projekts

A = Accountable. Die Person, für die R zuständig ist, muss Aktionen erst abzeichnen (Genehmiger), bevor sie akzeptiert werden.

C = Consulted. Die Person, die konsultiert wird und Informationen bzw. die notwendigen Fähigkeiten besitzt, um die Aktionen abzuschließen.

I = Informed. Die Person, die über die Ergebnisse verständigt werden muss, jedoch zuvor nicht konsultiert werden muss.

Einer der Hauptzwecke von CA RCM-RACI ist es, Entitätsmanager zu identifizieren (Genehmiger). Jede Modellkonfiguration, für die Sie ein Audit durchführen möchten, muss über den RACI-Generator durchgeführt werden, so dass die Genehmiger richtig aufgelistet werden.

Das RACI-Hilfsprogramm erhält die von Ihnen bei der Festlegung des Universums als Managerfelder identifizierten Datenfelder und kennzeichnet sie als "Accountables" des Systems. Die Daten des Benutzer-Managers werden aus der Benutzerdatenbank der Konfigurationsdatei (*.udb) entnommen. Jeder Benutzer kann "Accountable" für mehrere Entitäten sein, Entitäten haben jedoch nur eine einzige Person als "Accountable" zugewiesen.

Hinweis: Führen Sie das RACI-Hilfsprogramm aus, bevor Sie eine Kampagne starten, da das System keine Benutzer haben kann, die als "Accountables" für Entitäten festgelegt wurden. Somit können keine Genehmigertickets an die korrekten Entitätenmanager gesendet werden. Wenn Sie RACI nicht ausführen, wird entweder eine Fehlermeldung angezeigt oder alle Entitäten werden zur Genehmigung mit den Kampagneneingentümern aufgelistet.

Erstellen von RACI-Konfigurationsdateien

Sobald ein Universum erstellt ist, erstellen Sie seine RACI-Konfigurationen. Über die RACI-Konfigurationen werden die Zuweisungen von Zertifikations-, Nachweis- oder Genehmigungsaufgaben für den entsprechende "Accountable" kontrolliert. Es sind vier RACI-Konfigurationen vorhanden, eine pro Person (R, A, C, I). CA RCM erstellt die A-Konfiguration automatisch und greift dabei auf den Inhalt der Felder "Eigentümer" oder "Manager" des Universums zurück.

Hinweis: Aktualisieren Sie die CA RCM-Benutzerdatenbank, bevor Sie RACI für das Universum erstellen.

So erstellen Sie RACI-Konfigurationsdateien

1. Klicken Sie im Menü "Verwaltung" auf "RACI erstellen".

   Das Konfigurationsfenster "RACI erstellen" wird geöffnet.

2. Wählen Sie ein Universum in der Dropdown-Liste aus.

3. Klicken Sie auf "RACI erstellen".

   Ein entsprechender Hinweis wird angezeigt, wenn der Prozess abgeschlossen ist.

Hinweis: Wenn die RACI-Konfigurationsdateien beschädigt sind, können Sie über das CA RCM-DNA-Modul zugreifen. Klicken Sie im Menü "Datei" auf "Review Database" (Datenbank überprüfen). Danach können die Dateien angezeigt oder gelöscht werden.

Synchronisieren von RACI

Sie müssen die RACI-Konfigurationen regelmäßig aktualisieren, sodass sie am Universum vorgenommene Änderungen widerspiegeln.

Hinweis: Wenn Sie neue Benutzerdatensätze in die Konfigurationsdateien des Universums importieren, kann sie der Datenconnector automatisch (siehe Seite 214) zu den RACI-Konfigurations-Dateien des Universums zuordnen.

Standardmäßig fügt die RACI-Synchronisierung neue Entitätsdaten hinzu oder löscht Entitäten, die nicht mehr im Universum existieren, aber es aktualisiert vorhandene Verknüpfungen in den RACI-Konfigurationen nicht. Die folgenden Systemeigenschaften ermöglichen es der RACI-Synchronisierung, vorhandene Verknüpfungen zu aktualisieren:

raci.sync.override.accountable.roles

Bestimmt, ob vorhandene Rollen in der "Accountable"-Konfiguration aktualisiert werden. Wenn diese Boolesche Eigenschaft wahr ist, wird die "Accountable"- Konfiguration aktualisiert, wenn der "Accountable"-Benutzer sich für eine Rollenentität ändert. Um diese Eigenschaft für ein Universum zu implementieren, erstellen Sie eine neue Eigenschaft mit dem folgenden Namen:

`universe.property.`*`universe_name`*`.raci.sync.override.accountable.roles`

Hinweis: "*universe_name*" ist der Name des Zieluniversums.

raci.sync.override.accountable.resources

Bestimmt, ob vorhandene Ressourcen in der "Accountable"-Konfiguration aktualisiert werden. Wenn diese Boolesche Eigenschaft wahr ist, wird die "Accountable"- Konfiguration aktualisiert, wenn der "Accountable"-Benutzer sich für eine Ressourcenentität ändert. Um diese Eigenschaft für ein Universum zu implementieren, erstellen Sie eine neue Eigenschaft mit dem folgenden Namen:

`universe.property.`*`universe_name`*`.raci.sync.override.accountable.roles`

Hinweis: "*universe_name*" ist der Name des Zieluniversums.

So synchronisieren Sie RACI-Konfigurationsdateien

1. Gehen Sie im CA RCM-Portal zu "Verwaltung", "Berechtigungen" und "RACI", "RACI Synchronisieren".

   Das Fenster "RACI-Konfigurationen synchronisieren" erscheint.

2. Wählen Sie in der Dropdown-Liste ein Universum aus, und klicken Sie auf "RACI synchronisieren".

   CA RCM aktualisiert die RACI-Konfigurationsdateien des Universums.

Systemüberprüfung

Verwenden Sie CA RCM-Systemüberprüfungs-Tools, um sicherzustellen, dass Nachrichtenbehandlungsprozesse richtig funktionieren.

Die Systemüberprüfungsoption ermöglicht es Ihnen, die folgenden E-Mail-Systeme zu überprüfen:

SMTP-Überprüfung

Überprüfen Sie Simple-Mail-Transfer Protocol-Kommunikation mit einem E-Mail-Server in der Umgebung.

Workpoint-Überprüfung

Überprüfen Sie die Kommunikation mit dem Workpoint-Server.

JMS-Warteschlangenüberprüfung

Überprüfen Sie die Kommunikation via Java Messaging Service.

SMTP-Überprüfung

Für die E-Mail-Verbindungen des TMS wird Simple Mail Transfer Protocol verwendet.

So überprüfen Sie die SMTP-Kommunikation

1. Gehen Sie im CA RCM-Portal auf "Verwaltung", "Systemüberprüfung", "SMTP-Überprüfung".

   Das Fenster "Überprüfungsoptionen" öffnet sich.

2. Geben Sie eine Ziel-E-Mail-Adresse ein.

3. Klicken Sie auf "Senden".

   Eine E-Mail wird von dem in der Systemeigenschaft "mail.from" angegebenen Sender an die Zieladresse gesendet.

4. Überprüfen Sie, ob die E-Mail eingetroffen ist.

Workpoint-Überprüfung

Die Workpoint-Überprüfung ermöglicht es Ihnen, den TMS-Workpoint-Adapter zu bearbeiten, die Workpoint-Prozessliste anzuzeigen und ein Überprüfungsticket zu starten.

Die Schaltfläche "Bearbeiten" erlaubt es Ihnen, den TMS-Workpoint-Adapter, der die Datenkommunikation mit dem Workpoint-Server verwaltet, zu bearbeiten Sie können den TMS-Eigenschaftsschlüsselwert bearbeiten und ins Fenster "Eigenschaft bearbeiten" Text eingeben. Sie können auch den Eigenschaftsschlüssel aus der Datenbank entfernen.

Die Schaltfläche "Start" ermöglicht es Ihnen, aktive Prozesse mit Überprüfungstickets zu starten, die in der Liste "Workpoint-Prozesse" angezeigt werden.

JMS-Warteschlangenüberprüfung

Die Java Message Service-Überprüfung ermöglicht es Ihnen, die JMS-Konnektivität zu testen.

Sie können entscheiden, ob Sie die Meldung sofort, mit einer benutzerdefinierten Verzögerung in Sekunden, oder in manuellem Modus empfangen möchten.

Datensätze und Meldungen werden angezeigt.

Extrahieren von CA RCM-Daten

Sie können CA RCM-Daten in die externe Berichtsdatenbank von CA RCM extrahieren. Anwendungen zur Berichterstattung und Data Mining von Dritten können auf diese Datenbank zugreifen, um Berichte zu generieren oder Analysen durchzuführen. Jeder extrahierte Daten-Snapshot stellt eine statische Kopie von CA RCM-Objekten dar. CA RCM aktualisiert die Daten-Snapshots nicht, nachdem sie erstellt wurden.

Wenn Sie mit Datenextraktion arbeiten, führen Sie folgende Vorgänge aus:

- Sie aktivieren Sie die externe Berichtsdatenbank (siehe Seite 278). Sie erstellen die Datenbank und aktivieren die Funktion auf dem CA RCM-Server.
- Sie erstellen ein Extraktionsprofil (siehe Seite 279), das die Art der Datendateien definiert, die in die externe Berichtsdatenbank kopiert werden.
- Sie generieren einen Datensatz oder Snapshot (siehe Seite 280) auf der Basis eines Extraktionsprofils. Sie können die automatische Generierung eines Datensatzes zu einem festen Zeitpunkt oder in wiederkehrenden Intervallen planen. Jeder Datensatz ist mit dem zu seiner Generierung verwendeten Profilnamen und einem Zeitstempel gekennzeichnet.
- Verfolgen Sie Datenextraktionsjobs (siehe Seite 281)-Datenextraktionsjobs werden im Posteingang des Verwaltungsadministrators angezeigt.
- Löschen Sie Profil- und Daten-Snapshots (siehe Seite 282), wenn sie nicht mehr gebraucht werden. Sie können individuelle Datensätze löschen oder ihre Löschung für einen zukünftigen Zeitpunkt planen.

Extraktionsprofile sind den Datenconnectors ähnlich. Im Tool zur Jobplanung des Portals können Sie Daten-Snapshots wie Datenconnectorjobs initiieren.

Die Datenstruktur der externen Berichtsdatenbank befindet sich in der Datei **CA-RCM-*rel#*-Language-Files.zip** des CA RCM-Installationspakets.

Aktivieren von externen Berichtsdatenbanken

Extrahierte Daten werden in einer speziell dafür vorgesehenen Microsoft SQL Server-Datenbank gespeichert. Führen Sie die folgenden Schritte durch, um die externe Berichtsdatenbank zu aktivieren:

1. Erstellen Sie die Datenbank auf einem Microsoft SQL Server folgendermaßen:

   - Wenn ein Microsoft SQL Server CA RCM-Datenbanken hostet, wählen Sie die Option "Externe Berichtsdatenbank" im CA RCM-Installationsprogramm aus, um diese Datenbank automatisch zu erstellen.

   - Wenn ein Oracle-Datenbankserver CA RCM-Datenbanken hostet, erstellen Sie die externe Berichtsdatenbank auf einer Microsoft SQL Server-Instanz, nachdem Sie CA RCM installiert haben.

   Hinweis: Weitere Informationen zur Erstellung von externen Berichtsdatenbanken finden Sie im *Installationshandbuch*.

2. Um die Datenextraktion zu aktivieren, setzen Sie den folgenden CA RCM-Systemparameter auf "True" (Wahr).

   reportdb.enabled

   Gibt an, ob CA RCM Datensnapshots in der externen Berichtsdatenbank speichert.

   Gültige Werte: True, False (Wahr, Falsch)

   Hinweis: CA RCM setzt diese Eigenschaft wieder auf "False" (Falsch) zurück, wenn ein geplanter Datensnapshot nicht in die Datenbank exportiert werden kann. Wenn die Verbindung zum Datenbankserver unterbrochen wird, wird die Eigenschaft auf "True" (Wahr) zurückgesetzt, wenn die Verbindung wiederhergestellt wird.

Erstellen von Datenextraktionsprofils

Erstellen Sie ein Profil, das festlegt, welche CA RCM-Daten in die externe Berichtsdatenbank kopiert werden.

Hinweis: Sie benötigen Administrator-Berechtigungen im CA RCM-Portal, um diesen Vorgang auszuführen.

So erstellen Sie ein Datenextraktionsprofil

1. Klicken Sie im Hauptmenü des Portals auf "Verwaltung" und anschließend auf "Externe Berichtsdatenbank".

   Das Hauptfenster "Externe Berichtsdatenbank" wird angezeigt.

2. Klicken Sie auf "Neues Profil".

   Hinweis: Um ein bestehendes Exportprofil zu bearbeiten, klicken Sie in der Profilliste auf seinen Namen.

   Das Fenster "Basisinformationen" wird angezeigt.

3. Geben Sie einen Namen und eine kurze Beschreibung des Profils ein und klicken Sie auf "Weiter".

   Das Parameterfenster wird angezeigt. Alle Dateien und Datenobjekte der CA RCM-Datenbanken werden nach Typ aufgelistet.

4. Klicken Sie auf jede Registerkarte und wählen Sie die Datendateien aus, die Sie in die extrahierten Daten miteinschließen möchten.

5. (Optional) Klicken Sie auf die Registerkarte "Tickets", und wählen Sie die Option "Alle Tickets" aus, um die gesamte Ticketdatenbank zu exportieren.

   Hinweis: Wenn Sie eine Kampagne auswählen, werden alle verwandten Tickets in den Daten-Snapshot aufgenommen, selbst wenn Sie die Option "Alle Tickets" nicht auswählen.

6. Klicken Sie auf "Next".

   Das Fenster "Übersicht" wird geöffnet.

7. Überprüfen Sie die Profildefinition.

8. Klicken Sie auf "Fertig stellen".

   Das Profil wird erstellt. Das Hauptfenster "Externe Berichtsdatenbank" wird angezeigt. Das neue Profil wird in der Profilliste angezeigt.

Ausführen und Planen von Datenextraktionsjobs

Der Datenextraktionsjob speichert die Dateien basierend auf einem Extraktionsprofil in die externe Berichtsdatenbank. Definieren Sie mindestens ein Extraktionsprofil, bevor Sie einen Datenextraktionsjob ausführen.

Sie können einen einzelnen Daten-Snapshot generieren oder die Generierung von Daten-Snapshots in regelmäßigen Zeitabständen planen.

Wenn Sie einen Datenextraktionsjob ausführen, wird ein Verfolgungsticket in Ihrem Posteingang angezeigt.

Hinweis: Sie benötigen Administrator-Berechtigungen im CA RCM-Portal, um diesen Vorgang auszuführen.

So führen Sie Datenextraktionsjobs aus oder planen sie.

1. Klicken Sie im Hauptmenü des Portals auf "Verwaltung" und anschließend auf "Externe Berichtsdatenbank".

   Das Hauptfenster "Externe Berichtsdatenbank" wird angezeigt.

2. Wählen Sie *eine* der folgenden Optionen aus:

   - Klicken Sie in der Profilliste, in der Zeile des Extraktionsprofils, das der Job verwenden soll, auf "Jetzt ausführen".

     Der Job wird sofort gestartet.

   - Um weitere Ausführungen eines Jobs zu planen, klicken Sie in der Profilliste, in der Zeile des Extraktionsprofils, das der Job verwenden soll, auf "Ablaufplan".

     Das Dialogfeld "Extraktionsaufgabe planen" wird angezeigt.

     Füllen Sie die folgenden Felder aus:

     - **Erste Ausführung** – Gibt Datum und Uhrzeit für die erste Ausführung des Jobs an.
     - **Anzahl der zusätzlichen Wiederholungen** - Anzahl der Ausführungen eines Jobs. Geben Sie den Wert -1 ein, um eine unendliche Reihe festzulegen.
     - **Wiederholungsintervall** – Zeitraum zwischen den Ausführungen der Reihe.

3. Klicken Sie auf "OK".

   Der Ablaufplan wird gespeichert. CA RCM initiiert nach Ablaufplan automatisch Daten-Snapshots.

Verfolgen von Datenextraktionsjobs

Wenn Sie die Datenextraktion in die externe Berichtsdatenbank in CA RCM beginnen, wird ein Jobticket für die Berichtsdatenbank-Snapshot-Extraktion in Ihrem Posteingang angezeigt. Sie können dieses Ticket dazu verwenden, die Generierung eines Daten-Snapshots zu verfolgen.

Wenn Sie die Datenextraktion sofort starten, wird das Ticket unmittelbar in der Schlange angezeigt.

Wenn Sie eine Reihe von Daten-Snapshots planen, wird bei Beginn der Datenextraktion ein neues Ticket für jeden Snapshot angezeigt.

Sie können im Fenster "Jobplanung" auch geplante Datenextraktionsjobs überprüfen und löschen. Datenextraktionsjobs werden im Fenster "Jobplanung" mit einem Jobnamen aufgelistet:

EXTRACTION.*extractionJobDetail*

Die Jobklassenbeschreibung hat den Wert **ExtractionJob**.

Hinweis: Sie benötigen Administrator-Berechtigungen im CA RCM-Portal, um diesen Vorgang auszuführen.

So verfolgen Sie Datenextraktionsjobs

1. Führen Sie einen Datenextraktionsjob im CA RCM-Portal aus oder planen Sie ihn.
2. Klicken Sie im Hauptmenü auf den Posteingang.

   Das Fenster "Posteingang" wird angezeigt: Wenn ein Datenextraktionsjob aktiv ist, wird ein Berichtsdatenbank-Snapshot-Extraktionsticket in der Warteschlange angezeigt. Der Tickettitel entspricht dem Namen des Datenexportprofils, auf dem der Job basiert.
3. Klicken Sie auf den Tickettitel

   Das Ticket wird geöffnet.

   Das Ticket enthält die folgenden Standardabschnitte:

   - Im Standard-Ticket-Header werden Informationen zur Identifikation und zum Status angezeigt
   - Der Abschnitt "Weitere" enthält Informationen zu Priorität, Schweregrad und Ticketverlauf.
   - In Abschnitt "Erweitert" können Sie Anhänge und Hinweise hinzufügen.

4. Überprüfen Sie die Tabelle im Abschnitt "Extraktionskomponenten", um den Jobfortschritt zu verfolgen.

   In jeder Reihe der Tabelle wird ein CA RCM-Datentyp aufgelistet, sowie die Zeit, die benötigt wird, um alle Dateien des von Ihnen ausgewählten Typs zu exportieren. Wenn die Extraktion vollständig ist, zeigt das Feld "Extraktionsstatus" für alle Datentypen den Wert BEENDET an.

5. Öffnen Sie den Abschnitt "Extraktionsparameter für das Profil", um den Umfang des Extraktionsjobs zu überprüfen.

   Die Tabelle listet die Datentypen auf, die im Datenexportprofil enthalten sind, das für diesen Job verwendet wird, sowie die Anzahl an Datendateien jedes Typs, die zum Export ausgewählt wurden.

6. Klicken Sie auf "Bestätigen", wenn die Extraktion aller Datentypen abgeschlossen ist.

   Der Ticketstatus wechselt zu "Abgeschlossen" und das Ticket wird von der aktiven Ticket-Warteschlange entfernt.

Löschen von Datenextraktionsprofilen oder Daten-Snapshots

Regelmäßig geplante Datenextraktionen können ein großes Datenvolumen generieren. Löschen Sie ältere Datensätze, um die Größe der externen Berichtsdatenbank CA RCM zu reduzieren. Sie können auch eine automatische Löschung für einen zukünftigen Tag und Zeitpunkt planen.

Ähnlich dazu können Sie ein Datenexportprofil löschen, wenn der Datensatz, den es definiert, nicht länger gebrauchen wird.

Hinweis: Sie benötigen Administrator-Berechtigungen im CA RCM-Portal, um diesen Vorgang auszuführen.

So löschen Sie Datenextraktionsprofile oder Daten-Snapshots

1. Klicken Sie im Hauptmenü des Portals auf "Verwaltung" und anschließend auf "Externe Berichtsdatenbank".

   Das Hauptfenster "Externe Berichtsdatenbank" wird angezeigt.

2. (Optional) Löschen Sie ein Extraktionsprofil:

   a. Suchen Sie ein Exportprofil, das Sie aus der Profilliste löschen möchten.

   b. Klicken Sie in der Zeile des Exportprofils auf "Löschen".

      Das Extraktionsprofil wird gelöscht.

3. (Optional) Löschen Sie einen Daten-Snapshot:

   a. Suchen Sie in der Snapshot-Liste einen Datensatz, den Sie löschen möchten.

   b. Klicken Sie in der Zeile des Datensatzes auf "Löschen".

      Der Datensatz wird gelöscht.

4. (Optional) Planen Sie weitere Löschungen von Daten-Snapshots:

   a. Suchen Sie in der Snapshot-Liste einen Datensatz, den Sie löschen möchten.

   b. Klicken Sie in der Zeile des Datensatzes auf "Löschen planen".

      Das Dialogfeld "Löschen des Snapshots planen" wird angezeigt.

   c. Legen Sie das Datum und den Zeitpunkt fest, zu dem der Snapshot gelöscht werden soll, und klicken Sie auf OK.

      Der Snapshot wird zum geplanten Datum und Zeitpunkt gelöscht.

Kapitel 13: Sicherheit und Berechtigungen

Die Sicherheit eines Unternehmens hat enorme Auswirkungen, besonders wenn man die möglichen Schäden in Betracht zieht, die durch Verlust, Änderungen durch nicht autorisierte Benutzer oder Missbrauch von Daten und Ressourcen verursacht werden können.

Das CA RCM-Portal ist zugänglich für Senior-Administratoren sowie für gewöhnliche Benutzer. Diese unterschiedlichen Typen von Benutzern haben unterschiedliche Bedürfnisse und nutzen CA RCM auf unterschiedliche Weisen. Unter Verwendung des Portals können Sie rollenbasierte Sicherheit und Berechtigungen definieren, um entsprechende Sicherheitsebenen aufrechtzuerhalten.

Dieses Kapitel enthält folgende Themen:

Sicherheit

Softwaresicherheit soll sowohl versehentlicher als auch böswilliger Beschädigung vorbeugen. Es gibt verschiedene Wege, um dieses Ziel zu erreichen. Dieser Abschnitt enthält die Lösungen des CA RCM-Portals für bestimmte Sicherheitsprobleme.

Weitere Informationen:

Aktivieren der Sicherheit (siehe Seite 286)
Authentifizierungseinstellungen (siehe Seite 286)
Verschlüsselung (siehe Seite 287)

Aktivieren der Sicherheit

Software-Sicherheit kann so konfiguriert werden, dass sie sich auf eine der folgenden Weisen verhält:

Standard: Verweigern

Unter diesen Bedingungen ist alles unzulässig, das nicht ausdrücklich genehmigt ist. Während diese Methode die Sicherheit verbessern kann, kann sie sich negativ auf die Funktionalität auswirken.

Standardgenehmigung

Alles ist genehmigt. Der Vorteil dieser Art von Sicherheitsoperation besteht darin, dass sie mehr Funktionen ermöglicht. Sie könnte sich für die Anfangsphasen des Einrichtens und Systemtestens eignen.

Standardmäßig wird Sicherheit im CA RCM-Portal deaktiviert. Wenn ein Benutzer sich mit einem anerkannten Benutzernamen anmeldet, überprüft das CA RCM-Portal die Benutzerberechtigungen nicht und es gibt keine Grenzen dafür, was der Benutzer sehen und ausführen kann.

Sie konfigurieren den Typ von Sicherheit, der in dem CA RCM-Portal verwendet wird, indem Sie einen Sicherheitsparameter in der "eurekify.properties"-Datei festlegen.

Der Sicherheitsparameter ähnelt dem Folgenden:

```
sage.security.disable=true
```

Wird für diese Eigenschaft "falsch" festgelegt, wechselt CA RCM zur Sicherheitsmethode "Default Deny". Nur Funktionalitäten, die explizit erlaubt sind, sind für den Benutzer sichtbar und aktiviert.

Weitere Informationen:

Berechtigungen (siehe Seite 288)

Authentifizierungseinstellungen

Authentifizierung bedeutet, festzustellen, dass ein Benutzer hinreichende Sicherheitsberechtigungen hat, um auf das CA RCM-Portal zuzugreifen. Der folgende Sicherheitsparameter, der sich in der "eurekify.properties"-Datei befindet, entscheidet, ob Benutzer ein Kennwort benötigen, um auf das CA RCM-Portal zuzugreifen:

```
sage.security.disable.ADAuthentication=true
```

Wird für diese Eigenschaft "wahr" festgelegt, muss der Benutzer sein registriertes Kennwort nicht verwenden, um sich am CA RCM-Portal anzumelden. Statt dessen erlaubt ihm eine beliebige alphanumerische Zeichenfolge den Zugang.

Wird für die Eigenschaft "falsch" festgelegt, müssen Benutzer ein registriertes Kennwort angeben, um auf das CA RCM-Portal zuzugreifen.

Kennwörter werden in einem unternehmenseigenen Active Directory-Server gespeichert. Wenn ein Benutzer sich anzumelden versucht, werden Benutzername und Kennwort zur Authentifizierung an den Active Directory-Server gesendet.

Verschlüsselung

Beim Senden der Benutzeranmelde- und Kennwortdaten wird empfohlen, diese Daten zu verschlüsseln. Die in der "eurekify.properties"-Datei anzutreffenden Sicherheitsparameter lauten wie folgt:

```
sage.security.disable.ssl.ADAuthentication=true
```

Lautet der Wert für diesen Parameter "wahr", wird die Secure Sockets Layer (SSL)-Authentifizierung deaktiviert.

Wenn für den Parameter der Wert "falsch" festgelegt und die SSL-Verschlüsselung aktiviert wird, müssen Sie die Schlüsselspeicherdatei im folgenden Sicherheitsparameter liefern:

```
sage.security.eurekify.keyStore.file=
```

Die Schlüsselspeicher-Datei ist eine Datenbank, in der die privaten und öffentlichen Schlüssel gespeichert werden, die für SSL-Verschlüsselung und -Entschlüsselung notwendig sind.

Berechtigungen

Wenn die Sicherheit aktiviert ist, wird jede Aktion, die ein Benutzer auszuführen versucht, mit dessen Berechtigungen abgeglichen.

Um die Sicherheit in CA RCM zu aktivieren, bearbeiten Sie die Berechtigungskonfigurationsdatei (eurekify.cfg). Jede Rolle in dieser Konfigurationsdatei repräsentiert eine Reihe von Berechtigungen. Jede Ressource in der Konfigurationsdatei ist eine Regel oder ein Filter, der den Inhalt und Umfang des Zugriffs auf Portalfunktionen oder -daten definiert. Um einem Benutzer Berechtigungen zu geben, verbinden Sie die entsprechenden Ressourcen mit einer Rolle und stellen Sie sicher, dass der Benutzer ein Mitglied dieser Rolle ist.

Es gibt keine Berechtigungsfilter für Delegierungs- oder Eskalationsfunktionen.

Hinweis: Ein Genehmiger kann die Inhalte eines Genehmigertickets anzeigen, auch wenn ein Administrator dem Genehmiger die entsprechenden Berechtigungen nicht gegeben hat. CA RCM definiert Ressourcen, um dieses Problem im Hintergrund zu bearbeiten. Diese Berechtigungen sind auf diese spezifische Kampagnenanforderung beschränkt.

Weitere Informationen:

Die Berechtigungskonfigurationsdatei (siehe Seite 289)

Die Berechtigungskonfigurationsdatei

Um Berechtigungen für CA RCM zu verwalten, erstellen Sie zuerst mit dem DNA Client-Tool Ressourcen in der Berechtigungskonfigurationsdatei (eurekify.cfg). Die folgenden Typen von Ressourcen werden in CA RCM vordefiniert:

- Ressourcen vom Typ "Link". Sie bestimmen, welche Menüoptionen für jeden Benutzer sichtbar sind.
- Ressourcen vom Typ "Doc_Access". Sie entscheiden über den Zugriff auf CA RCM-Dokumentdateien, wie Konfigurationen, Auditkarten, Universen usw.
- Ressourcen vom Typ "Filter". Sie entscheiden über den Zugriff auf spezifische CA RCM-Entitäten.

So erstellen Sie Ressourcen in der Berechtigungskonfigurationsdatei (eurekify.cfg)

1. Vergewissern Sie sich, dass der Datenbankserver und der CA RCM-Server ausgeführt werden.
2. Ausführen des DNA Client Tools
3. Klicken Sie auf "Datei", "Datenbank überprüfen".

   Der Datenbankassistent öffnet sich.
4. Wählen Sie die "Eurekify.cfg"-Datei aus, entfernen Sie das Häkchen aus dem Kontrollkästchen "Schreibgeschützt", klicken Sie auf "Öffnen".

   Die "Eurekify.cfg"-Datei wird angezeigt. Jede Rolle in dieser Konfigurationsdatei repräsentiert eine Reihe von Berechtigungen. Jede Ressource ist eine Regel oder ein Filter, der den Inhalt und Umfang des Zugriffs auf Portalfunktionen oder -daten definiert.
5. Klicken Sie auf das Symbol "Ressourcen-Datenbank" oder klicken Sie auf "Anzeigen", "Ressourcen-Datenbank".

   Die mit der Konfiguration assoziierte Ressourcendatenbank wird in einem neuen Fenster angezeigt.
6. Klicken Sie im Ressourcendatenbankfenster mit der rechten Maustaste und wählen Sie "Ressource hinzufügen" aus.

   Das Fenster "Ressourcen-Details" wird angezeigt.
7. Füllen Sie die Felder entsprechend aus, je nach dem Ressourcentyp, den Sie hinzufügen (Link, Doc_Access, oder Filter.)
8. Klicken Sie auf "OK".
9. Wiederholen Sie die Schritte 6 bis 8 für jede Ressource, die Sie hinzufügen möchten.

10. Fügen Sie die neuen Ressourcen folgendermaßen zur Konfigurationsdatei hinzu:
    a. Wählen Sie eine neue Ressource aus und ziehen Sie sie zum Ressourcenabschnitt des "Eurekify.cfg"-Fensters.

       Der Cursor ändert sich in ein Symbol "HINZUFÜGEN".
    b. Lassen Sie den Cursor los.

       Die neuen Ressourcen werden der Konfigurationsdatei hinzugefügt.
11. Speichern Sie die Änderungen in der Datei "Eurekify.cfg".

Ressourcen des Typs "Link"

Ressourcen vom Typ "Link" bestimmen, welche Menüoptionen für jeden Benutzer sichtbar sind.

Die allgemeine Syntax lautet wie folgt:

```
[<Menüname>.<Untermenü>]
```

Geben Sie die Ressourcensyntax in den Res-Namen 1 Feld ein.

Zum Beispiel: [Self-Service.*] erteilt Benutzern, die mit dieser Ressource verknüpft sind, die Berechtigung dazu, alle verfügbaren Self-Service-Menüelemente anzuzeigen und zu verwenden.

Durch Hinzufügen von [EX]] nach den eckigen Klammern wird ein bestimmtes Menü oder Menüelement aus den Menüoptionen des Benutzers ausgeschlossen.

Um den Menüpunkt "Neue Rolle anfordern" auszuschließen, verwenden Sie zum Beispiel die folgende Syntax:

```
[SelfService.requestNewRole][EX]
```

Ressourcen des Typs Doc_Access

Ressourcen vom Typ "Doc_Access" entscheiden über den Zugriff auf CA RCM-Dokumentdateien, wie Konfigurationen, Auditkarten, Universen usw.

Die allgemeine Syntax lautet wie folgt:

```
[<Dokumenttyp>]
```

Geben Sie die Ressourcensyntax in den Res-Namen 1 Feld ein.

Zum Beispiel: [AUDITKARTE] erteilt Benutzern, die mit dieser Ressource verknüpft sind, die Berechtigung, auf diesen Dateityp zuzugreifen.

Durch Hinzufügen des Modifikators Read ([R]) oder Read/Write ([RW]) wird die Zugangsebene zu den Dateien festgelegt, auf die der Benutzer zugreifen darf.

Der Wert, der in die Spalte "Ressourcenname 2" eingegeben wird, beeinflusst die Berechtigungsebene. Ein Sternchen (*) zeigt vollständige Berechtigungen für alle solche Dateien an, oder es kann eine spezifische Entität, wie z. B. Konfigurationsname, Universumsname usw. aufgelistet werden.

Filtertyp-Ressourcen

Filter-Ressourcen bestimmen den Zugriff auf spezifische CA RCM-Entitäten. Filter beruhen auf dem standardmäßigen LDAP-Filter-Format.

Wenn Sie CA RCM eine Filter-Ressource hinzufügen, können Sie den folgenden Filter verwenden:

- [Filter_Benutzer]
- [Filter_Rolle]
- [Filter_Ressource]

Füllen Sie die folgenden zusätzlichen Felder auf, wenn Sie eine Filter-Ressource verwenden:

Ressourcenname 1

Gibt den zu verwendenden Filter an: Filter_User, Filter_Role, oder Filter_Resource.

Ressourcenname 2

Gibt den Universumsnamen an.

Ressourcenname 3

Gibt Filternamen oder -nummer an.

Beschreibung

Bietet eine Beschreibung des Filters.

Typ

Definiert den Ressourcentyp: Filter.

Filter1

Definiert den Filter. Zum Beispiel: (>(type=role)(A(type=user)(sageUser=$$PersonID$$))).

Filterformat

Filter beruhen auf dem LDAP-Präfixfilterformat. Der Filter wurde anhand eines Ausdrucks erstellt, der wiederum anhand von Unter-Ausdrücken erstellt worden sein könnte.

Jeder Filterausdruck wird von Klammern ("(",")") umgeben und repräsentiert eine Reihe von CA RCM-Entitäten.

Die einfachste Form eines Filters ist ein Feld/Wert-Paar, das aus einem CA RCM-Entitätsfeldnamen und dem gewünschten Wert, getrennt durch ein Gleichheitszeichen, besteht. Zum Beispiel: "(Location=Cayman)" oder "(PersonID=86.*)".

Ein anderer einfacher Filter ist (Name>Schmidt) der Benutzer zurückgibt, deren Namensfelder in alphabetischer Reihenfolge nach "Schmidt" auftreten. Somit gibt ein Filter wie der folgende:

```
(&(UserName>C)(UserName<F))
```

Benutzer zurück, deren Namensfeld zwischen die Buchstaben C und F fällt, einschließlich C und F selbst.

Ein weiterer einfacher Filter gibt Entitätsübereinstimmungen zurück. Dieser Filter fängt mit einer Tilde an (~) und ist ein Entität/Wert-Paar, das aus einem CA RCM-Entitätstyp besteht (Benutzer/Rolle/Ressource) und einem zugehörigen Entitätennamen, jeweils getrennt durch ein Gleichheitszeichen. Für Ressourcen erscheinen drei Klammernsätze mit den drei Paaren nach dem ~. Beispiel:

```
(~(Rolle=Kaiman)) oder (~(Ressourcenname1=E-
Mail)(Ressourcenname2=Outlook)(Ressourcenname3=WinNT))
```

Auf den Filter können auch logische Operationen angewendet worden sein. Es stehen AND, OR und NOT zur Verfügung. Operator-Symbole lauten folgendermaßen:

& - AND

| - OR

! – NOT

Operator-Symbole sind Präfixe und sollten vor den/die Ausdru(e)ck(e) gesetzt werden.

```
"(&(Location=Cayman)(Organization=Finance))" - Benutzer im Finanzbüro von Kaiman.
```

```
"(|(Country=US)(Country=UK))" - Personen in US oder UK.
```

```
"(!(Active=false))" - Aktive Benutzer.
```

Filter können so komplex wie notwendig sein, solange sie den weiter oben aufgelisteten Regeln entsprechen. Beispiel:

```
"(&(|(Country=US)(Country=UK))(&(!(Active=false))(Organization=Finance)))"
```

Dieser Filter gibt alle aktiven Benutzer zurück, die in US oder UK und in der Finanzabteilung sind.

Filtererweiterung

Diese Filtererweiterungen sind nur für den internen Gebrauch (Kampagnen). Die folgenden zusätzlichen Filter betreffen das RACI-Modell:

A - genehmigte Entitäten

> - Links zu genehmigten Entitäten

Beispiel:

- Alle Rollen, deren Genehmiger “AD1\Admin” ist

  ```
  (A(type=role)(sageUser=AD1\Admin))
  ```

- Alle mit Benutzern verknüpfte Rollen, deren Manager “AD1\Admin” ist

  ```
  (>(type=role)(A(type=user)(sageUser=AD1\Admin)))
  ```

Zuweisen einer Ressource zu einer Rolle

Weisen Sie einer Rolle Ressourcen zu, um Benutzern dieser Rolle Zugriff zu den definierten Portalberechtigungen zu gewähren.

So weisen Sie einer Rolle Ressourcen zu:

1. Wählen Sie im Eurekify.cfg-Fenster im DNA-Client-Tool neue Ressourcen aus und ziehen Sie sie auf eine der unter dem Rollen-Abschnitt des Fensters aufgelisteten Rollen.

   Der Cursor verwandelt sich in ein LINK-Symbol.

2. Lassen Sie den Cursor los.

   Die neuen Ressourcen sind mit der in Schritt 1 angegebenen Rolle verbunden.

3. Klicken Sie mit der rechten Maustaste auf die in Schritt 1 angegebene Rolle und wählen Sie "Alle verbundenen Entitäten anzeigen".

   Die mit der Rolle verbundenen Benutzer- und Ressourcen-Entitäten werden hervorgehoben.

   Hinweis: Wenn Sie einer Rolle Benutzer hinzufügen müssen, wählen Sie den Benutzer im Benutzer-Abschnitt des Eurekify.cfg-Fensters und ziehen Sie ihn auf eine der Rollen, die unter dem Rollen-Abschnitt des Fensters aufgelistet sind.

4. Vergewissern Sie sich, dass die neuen Ressourcen mit der in Schritt 1 angegebenen Rolle verbunden sind.
5. Speichern Sie Änderungen in der Datei "Eurekify.cfg".

Beispiel: Hinzufügen eines Filters, um einem Benutzer Self-Service-Zugriff zu gewähren

Um einem Benutzer Zugriff auf alle seine eigenen Entitäten für die Self-Service-Funktionalität zu gewähren, fügen Sie zu CA RCM die folgenden Filtertypenressourcen mithilfe des DNA-Client-Tools hinzu.

1. Fügen Sie einen Benutzerfilter hinzu, indem Sie das Fenster "Ressourcendetails" folgendermaßen ausfüllen:
   - Res Name 1: [FILTER_USER]
   - Res Name 2: *

- Beschreibung: Benutzer können sich in Universen sehen, die das Feld "Anmelde-ID" verwenden.
- Typ: Filter
- Filter1: (user.LoginID=$$PersonID$$)

2. Fügen Sie einen Rollenfilter hinzu, indem Sie das Fenster "Ressourcendetails" folgendermaßen ausfüllen:
   - Res Name 1: [FILTER_ROLE]
   - Res Name 2: *
   - Beschreibung: Benutzer können ihre eigenen Rollen in Universen sehen, die das Feld "Anmelde-ID" verwenden.
   - Typ: Filter
   - Filter1: (~(user.LoginID=$$PersonID$$))
3. Fügen Sie einen Ressourcenfilter hinzu, indem Sie das Fenster "Ressourcendetails" folgendermaßen ausfüllen:
   - Res Name 1: [FILTER_RES]
   - Res Name 2: *
   - Beschreibung: Benutzer können ihre eigenen Ressourcen in Universen sehen, die das Feld "Anmelde-ID" verwenden.
   - Typ: Filter
   - Filter1: (~(user.LoginID=$$PersonID$$))

   Hinweis: Um zu vermeiden, dass die Filterzeichenfolge abgeschnitten wird, machen Sie die Spalte "Filter1" im Fenster "Ressource bearbeiten" breiter, bevor Sie die Zeichenfolge eingeben.
4. Geben Sie für jeden neuen Ressourcenfilter in numerischer Folge einen Wert für die Filter-ID ein (Res Name 3).
5. Verbinden Sie die neuen Ressourcenfilter mit einer Rolle.
6. Speichern Sie die Änderungen in der Datei "Eurekify.cfg".

Wichtig! Wenn Sie das Anmelde-ID-Attribut zu einem anderen als dem Anmelde-ID im Universum zugeordnet haben, ändern Sie die Anmelde-ID entsprechend mit dem richtigen Attribut im Filter. Werden die Anmelde-IDs zum Beispiel im GUUID-Attribut gespeichert, ändern Sie den Filter folgendermaßen:

(user.GUUID=$$PersonID$$)

Kapitel 14: Fehlerbehebung

Dieses Kapitel stellt eine Liste der Fehlermeldungen des CA RCM-Portals zur Verfügung.

Dieses Kapitel enthält folgende Themen:

Fehlermeldungen

CA RCM enthält ein Nachrichtensystem, das dazu dient, eine Warnung auszugeben, wenn eine Aktivität nicht wie definiert abgeschlossen werden kann oder wenn weitere Informationen nötig sind, um die Aktivität abzuschließen: Die folgende Tabelle stellt typische Nachrichten sowie die auszuführende Aktion dar:

Feld	Code	Beschreibung
settings.raci.create.missingmanagers.errcode	adm001	Es wird empfohlen, dass alle Felder des Universum-Managers ausgefüllt werden, bevor RACI erstellt wird, damit die Accountable-Links automatisch hinzugefügt werden können.
settings.raci.create.alreadyexist.errcode	adm002	RACI-Konfigurationen sind für {0} bereits vorhanden
settings.raci.create.fail.errcode	adm003	RACI-Konfigurationen für {0} konnten nicht erstellt werden
required.errcode	app001	Feld ${label} ist erforderlich.
iconverter.errcode	app002	'${input}' ist kein gültiger ${type}.
numbervalidator.range.errcode	app003	${input} liegt nicht zwischen ${minimum} und ${maximum}.
numbervalidator.minimum.errcode	app004	'${input}' ist kleiner als der Mindestwert von ${minimum}.
numbervalidator.maximum.errcode	app005	'${input}' ist größer als der Maximalwert von ${maximum}.

Feld	Code	Beschreibung
numbervalidator.positive.errcode	app006	'${input}' muss positiv sein.
numbervalidator.negative.errcode	app007	'${input}' muss negativ sein.
stringvalidator.range.errcode	app008	'${input}' ist nicht zwischen ${minimum} und ${maximum} Zeichen lang.
stringvalidator.minimum.errcode	app009	'${input}' ist kürzer als der Mindestwert von ${minimum} Zeichen.
stringvalidator.maximum.errcode	app010	'${input}' ist länger als der Maximalwert von ${maximum} Zeichen.
stringvalidator.exact.errcode	app011	'${input}' ist nicht genau ${exact} Zeichen lang.
datevalidator.range.errcode	app012	'${input}' liegt nicht zwischen ${minimum} und ${maximum}.
datevalidator.minimum.errcode	app013	'${input}' ist weniger als der Mindestwert von ${minimum}.
datevalidator.maximum.errcode	app014	'${input}' ist größer als der Maximalwert von ${maximum}.
patternvalidator.errcode	app015	'${input}' entspricht nicht dem Muster '${pattern}'.
emailaddressvalidator.errcode	app016	'${input}' ist keine gültige E-Mail-Adresse.
creditcardvalidator.errcode	app017	Die Kreditkartennummer ist ungültig.
urlvalidator.errcode	app018	'${input}' ist keine gültige URL.
equalinputvalidator.errcode	app019	'${input0}' von ${label0} und '${input1}' von ${label1} müssen gleich sein.
equalpasswordinputvalidator.errcode	app020	${label0} und ${label1} müssen gleich sein.
user.count.roles.alert.description.errcode	apr001	Benutzer hat {0} Rollen
user.count.resources.alert.description.errcode	apr002	Benutzer hat {0} Ressourcen
role.count.users.alert.description.errcode	apr003	Rolle hat {0} Benutzer

Feld	Code	Beschreibung
role.count.children.alert.description.errcode	apr004	Rolle hat {0} untergeordnete Elemente
role.count.resources.alert.description.errcode	apr005	Rolle hat {0} Ressourcen
resource.count.users.alert.description.errcode	apr006	Ressource hat {0} Benutzer
resource.count.roles.alert.description.errcode	apr007	Ressource hat {0} Rollen
campaignchoicesvalidator.errcode	arp001	Wählen Sie mindestens eine Option für das Feld ${byfield} aus.
configurationname.required.errcode	arp002	Wählen Sie eine Konfiguration aus.
campaignname.required.errcode	arp003	Wählen Sie eine Kampagne aus.
byfield.required.errcode	arp004	Wählen Sie den Parameter 'Nach Feld'.
auditcard.required.errcode	arp005	Wählen Sie eine Auditkarte aus.
sort.required.errcode	arp006	Wählen Sie eine Sortiermethode aus.
campaignfilteroption.required.errcode	arp007	Wählen Sie einen Filtertyp aus.
campaign.sendreminder.error.errcode	cmp001	"Erinnerungen versenden" wurde abgebrochen, E-Mail-Ereignis ist nicht aktiv. Mailing-Parameter [tms.configuration.mail.events] in eurekify.properties aktualisieren
campaign.text.campagin.errors.found.errcode	cmp002	Gefundene Fehler
campaign.error.nouniversesavilable.errcode	cmp003	Es stehen keine Universen zur Verfügung.
campaign.error.missingcampaigndescription.errcode	cmp004	Kampagnenbeschreibung fehlt
campaign.error.missingenddate.errcode	cmp005	Enddatum fehlt
campaign.error.duedatemustbeinthefuture.errcode	cmp006	Fälligkeitsdatum muss in der Zukunft liegen
campaign.error.configurationmustbeselected.errcode	cmp007	Konfiguration muss ausgewählt sein
campaign.error.racinotavailablefor.errcode	cmp008	RACI nicht verfügbar für ({0})
campaign.error.campaignalreadyexists.errcode	cmp009	Kampagne [{0}] ist bereits vorhanden
campaign.error.noaccess.errcode	cmp010	Benutzer {0} hat keinen Zugriff auf Kampagne {1}

Feld	Code	Beschreibung
settings.strings.ie.errors.missingname.errcode	cst001	Feld 'Name' fehlt.
settings.strings.ie.errors.missingdescription.errcode	cst002	Feld 'Beschreibung' fehlt.
settings.strings.ie.errors.namealreadyexist.errcode	cst003	doppelter Name, Name wird bereits verwendet.
settings.strings.ie.errors.missinguniverse.errcode	cst004	Feld 'Universum' fehlt.
settings.strings.ie.errors.missingsettings.errcode	cst005	XML-Einstellungsdatei {0} nicht gefunden.
settings.strings.ie.errors.missingmapping.errcode	cst006	XML-Zuordnungsdatei {0} nicht gefunden.
settings.strings.ie.errors.missingenrichment.errcode	cst007	Anreicherungsdatei {0} nicht gefunden.
settings.strings.ie.errors.missingpassword.errcode	cst008	Feld 'Kennwort' fehlt.
settings.strings.ie.errors.missingmaxduration.errcode	cst009	Feld 'Maximale Dauer' fehlt.
settings.strings.ie.errors.errorparsingmaxduration. Fehlercode	cst010	Fehler bei der Analyse des Feldes 'Maximale Dauer', verwenden Sie ganzzahlige Werte.
settings.strings.ie.errors.missingconnectorclientclass.errcode	cst011	Zu verwendende Klasse des Connectorclients fehlt.
settings.strings.ie.errors.missingworkflowprocess. Fehlercode	cst012	Workflow-Prozess fehlt.
settings.strings.ie.errors.missingtickettype.errcode	cst013	Tickettyp fehlt.
dashboard.compliance.error.noname.errcode	dbc001	Geben Sie die Namen aller Auditkarten ein.
dashboard.compliance.error.multiname.errcode	dbc002	Der Name {0} erscheint mehr als einmal
dashboard.compliance.error.nocard.errcode	dbc003	Geben Sie alle Auditkarten an
dashboard.compliance.error.multicard.errcode	dbc004	Auditkarte {0} erscheint mehr als einmal

Feld	Code	Beschreibung
dashboard.compliance.error.nobpralerts.errcode	dbc005	Auditkarte {0} hat keine BPR-Warnungen
entity.emptylist.errcode	eml001	Es wurde keine Übereinstimmung gefunden
mail.builder.createticket.sage.errticket.subject.errcode	mal001	Neues Fehlerticket, Titel:{3}
mail.builder.createticket.sage.errticket.body.errcode	mal002	Ein Fehlerticket (id
properties.errormsg.propertyalreadyexists.errcode	prp001	Die Eigenschaft [{0}] ist bereits vorhanden
properties.errormsg.unencryptedpropertyalreadyexists.errcode	prp002	Eine nichtverschlüsselte Eigenschaft [{0}] ist bereits vorhanden, entfernen Sie sie zunächst.
properties.errormsg.contcreateemptyproperty.errcode	prp003	es kann keine Eigenschaft mit einem leeren Schlüssel oder einem Schlüssel von Null erstellt werden.
loginpage.userauthentication.failed.errcode	prt006	Benutzer konnte nicht authentifiziert werden, Benutzername/Kennwort ungültig
loginpage.connecttoauthenticationservice.failed. Fehlercode	prt007	Verbindung zum Authentifizierungsdienst konnte nicht hergestellt werden. Wenden Sie sich an Ihren Systemadministrator.
loginpage.userauthentication.failed.sageadmin. Fehlercode	prt008	falsches Kennwort für den Admin-Benutzer.
loginpage.userauthentication.failed.sagebatch.errcode	prt009	falsches Kennwort für den Batch-Benutzer.
loginpage.userauthorization.failed.errcode	prt010	Benutzer {0} konnte nicht autorisiert werden. Der Benutzer ist in der Konfiguration {1} nicht vorhanden.
internalerrorpage.label.info1.errcode	prt011	Ein Fehler ist aufgetreten Weitere Informationen finden sie in der Protokolldatei.
internalerrorpage.label.info2.errcode	prt012	Zum erneuten Anmelden hier klicken

Feld	Code	Beschreibung
sagemaster.headers.foundconflicts.errcode	sgm001	Fehler! Konflikte im Anmeldefeld der Masterkonfiguration.
sagemaster.headers.countduplicates.errcode	sgm002	{0} doppelte Anmeldungen gefunden. Bitte Prüfen:
selfservice.error.loading.bpr.errcode	sls001	BPR-Datei [{0}] konnte nicht geladen werden, fahre ohne sie fort
selfservice.error.finding.bpr.errcode	sls002	Keine BPR-Datei definiert, fahre ohne sie fort
selfservice.error.finding.universe.errcode	sls003	Es stehen keine Universen zur Verfügung.
selfservice.error.starting.approval.errcode	sls004	Fehler beim Starten des Genehmigungsvorgangs
selfservice.validate.descriptionrequired.errcode	sls005	Das Feld 'Beschreibung' ist erforderlich
selfservice.validate.nouserisselected.errcode	sls006	Kein Benutzer ausgewählt
selfservice.validate.norequestsmade.errcode	sls007	Keine Anfragen gestellt.
selfservice.validate.missingraciconfigurations.errcode	sls008	RACI-Konfigurationen fehlen
selfservice.validate.errorgettingraciconfigurations. Fehlercode	sls009	Fehler beim Abrufen der RACI-Konfigurationen
selfservice.validate.missingaccountablefor.errcode	sls010	'Accountable' für {0} fehlt
selfservice.validate.racierrorfor.errcode	sls011	RACI-Fehler für: {0}
settings.headers.editimportexportpage.error.errcode	ste001	Fehler beim Abrufen des Connectorobjekts: {0}
settings.headers.edituniversepage.error.errcode	ste002	Fehler beim Abrufen des Connectorobjekts
changeapproval.child.remove.user.role.info.title.rejected.errcode	tkt001	Anfrage zum Entfernen der Rolle {1} von Benutzer {1} abgelehnt.
changeapproval.child.remove.user.role.info.title.failed.errcode	tkt002	Anfrage zum Entfernen der Rolle {0} von Benutzer {1} - fehlgeschlagen.
changeapproval.child.remove.user.role.notification .title.errcode	tkt003	Die Anfrage zum Entfernen der Rolle {1} von Benutzer {0} wird bereits bearbeitet.

Feld	Code	Beschreibung
changeapproval.child.add.user.resource.info.title .rejected.errcode	tkt005	Anfrage zum Hinzufügen der Ressource {1} zum Benutzer {1} abgelehnt.
changeapproval.child.add.user.resource.info.title .failed.errcode	tkt006	Anfrage zum Hinzufügen der Ressource {0} zum Benutzer {1} fehlgeschlagen.
changeapproval.child.add.user.resource.info .description.rejected.errcode	tkt007	Die Anfrage zum Hinzufügen der Ressource {1} zum Benutzer {0} wurde abgelehnt. Die Anfrage wurde von {3} an Universum {2} gesendet
changeapproval.child.add.user.resource.info .description.failed.errcode	tkt008	Die Anfrage zum Hinzufügen der Ressource {1} zum Benutzer {0} ist fehlgeschlagen. Die Anfrage wurde von {3} an Universum {2} gesendet
changeapproval.child.remove.user.resource.info .title.rejected.errcode	tkt009	Anfrage zum Entfernen der Ressource {1} von Benutzer {0} - abgelehnt.
changeapproval.child.remove.user.resource.info .title.failed.errcode	tkt010	Anfrage zum Entfernen der Ressource {1} von Benutzer {0} - fehlgeschlagen.
changeapproval.child.remove.user.resource.info .description.rejected.errcode	tkt011	Die Anfrage zum Entfernen der Ressource {1} von Benutzer {0} wurde abgelehnt. Die Anfrage wurde von {3} an Universum {2} gesendet.
changeapproval.child.remove.user.resource.info .description.failed.errcode	tkt012	Die Anfrage zum Entfernen der Ressource {1} von Benutzer {0} ist fehlgeschlagen. Die Anfrage wurde von {3} an Universum {2} gesendet.
changeapproval.child.remove.user.resource .notification.title.errcode	tkt013	Die Anfrage zum Entfernen der Ressource {1} von Benutzer {0} wird bereits bearbeitet.
changeapproval.child.remove.user.resource .notification.description.errcode	tkt014	Die Anfrage zum Entfernen der Ressource {1} von Benutzer {0} wird bereits bearbeitet. Die Anfrage wurde von {3} an Universum {2} gesendet.
changeapproval.child.add.role.role.info.title.rejec ted.errcode	tkt015	Anfrage zum Hinzufügen der Rolle {0} zur Rolle {1} abgelehnt.

Feld	Code	Beschreibung
changeapproval.child.add.role.role.info.title.faile d .errcode	tkt016	Anfrage zum Hinzufügen der Rolle {0} zur Rolle {1} fehlgeschlagen.
changeapproval.child.add.role.role.info.descriptio n .rejected.errcode	tkt017	Die Anfrage zum Hinzufügen der Rolle {0} zur Rolle {1} wurde abgelehnt. Die Anfrage wurde von {3} an Universum {2} gesendet.
changeapproval.child.add.role.role.info.descriptio n .failed.errcode	tkt018	Die Anfrage zum Hinzufügen der Rolle {0} zur Rolle {1} ist fehlgeschlagen. Die Anfrage wurde von {3} an Universum {2} gesendet.
changeapproval.child.add.role.role.notification.til e .errcode	tkt019	Die Anfrage zum Hinzufügen der Rolle {0} zur Rolle {1} wird bereits bearbeitet.
changeapproval.child.add.role.role.notification .description.errcode	tkt020	Die Anfrage zum Hinzufügen der Rolle {0} zur Rolle {1} wird bereits bearbeitet. Die Anfrage wurde von {3} an Universum {2} gesendet.
changeapproval.child.remove.role.role.info.title .rejected.errcode	tkt021	Anfrage zum Entfernen der Rolle {0} von Benutzer {1} abgelehnt.
changeapproval.child.remove.role.role.info.title.f ailed.errcode	tkt022	Anfrage zum Entfernen der Rolle {0} von Benutzer {1} fehlgeschlagen.
changeapproval.child.remove.role.role.info .description.rejected.errcode	tkt023	Die Anfrage zum Entfernen der Rolle {0} aus der Rolle {1} wurde abgelehnt. Die Anfrage wurde von {3} an Universum {2} gesendet
changeapproval.child.remove.role.role.info .description.failed.errcode	tkt024	Die Anfrage zum Entfernen der Rolle {0} aus der Rolle {1} ist fehlgeschlagen. Die Anfrage wurde von {3} an Universum {2} gesendet
changeapproval.child.remove.role.role.notificatio n.title.errcode	tkt025	Die Anfrage zum Entfernen der Rolle {0} aus der Rolle {1} wird bereits bearbeitet.
changeapproval.child.remove.role.role.notificatio n .description.errcode	tkt026	Die Anfrage zum Entfernen der Rolle {0} aus der Rolle {1} wird bereits bearbeitet. Die Anfrage wurde von {3} an Universum {2} gesendet.

Feld	Code	Beschreibung
changeapproval.child.add.role.resource.info.title .rejected.errcode	tkt027	Anfrage zum Hinzufügen der Ressource {1} zur Rolle {1} abgelehnt.
changeapproval.child.add.role.resource.info.title. failed.errcode	tkt028	Anfrage zum Hinzufügen der Ressource {0} zur Rolle {1} fehlgeschlagen.
changeapproval.child.add.role.resource.info .description.rejected.errcode	tkt029	Die Anfrage zum Hinzufügen der Ressource {1} zur Rolle {0} wurde abgelehnt. Die Anfrage wurde von {3} an Universum {2} gesendet
changeapproval.child.add.role.resource.info.desc ription.failed.errcode	tkt030	Die Anfrage zum Hinzufügen der Ressource {1} zur Rolle {0} ist fehlgeschlagen. Die Anfrage wurde von {3} an Universum {2} gesendet
changeapproval.child.add.role.resource.notificati on .title.errcode	tkt031	Die Anfrage zum Hinzufügen der Ressource {1} zur Rolle {0} wird bereits bearbeitet.
changeapproval.child.add.role.resource.notificati on .description.errcode	tkt032	Die Anfrage zum Hinzufügen der Ressource {1} zur Rolle {0} wird bereits bearbeitet. Die Anfrage wurde von {3} an Universum {2} gesendet.
changeapproval.child.remove.role.resource.info.t itle .rejected.errcode	tkt033	Anfrage zum Entfernen der Ressource {1} aus Rolle {1} - abgelehnt.
changeapproval.child.remove.role.resource.info.t itle .failed.errcode	tkt034	Anfrage zum Entfernen der Ressource {0} aus Rolle {1} fehlgeschlagen.
changeapproval.child.remove.role.resource.info .description.rejected.errcode	tkt035	Die Anfrage zum Entfernen der Ressource {1} aus Rolle {0} wurde abgelehnt. Die Anfrage wurde von {3} an Universum {2} gesendet.
changeapproval.child.remove.role.resource.info .description.failed.errcode	tkt036	Die Anfrage zum Entfernen der Ressource {1} aus Rolle {0} ist fehlgeschlagen. Die Anfrage wurde von {3} an Universum {2} gesendet.
changeapproval.child.remove.role.resource .notification.title.errcode	tkt037	Die Anfrage zum Entfernen der Ressource {1} aus Rolle {0} wird bereits bearbeitet.

Feld	Code	Beschreibung
changeapproval.child.remove.role.resource .notification.description.errcode	tkt038	Die Anfrage zum Entfernen der Ressource {1} aus Rolle {0} wird bereits bearbeitet. Die Anfrage wurde von {3} an Universum {2} gesendet.
changeapproval.child.role.task.addroletoraci .description.errcode	tkt039	Um fortzufahren, wählen Sie bitte einen 'Accountable' für die Rolle {0} aus
changeapproval.child.remove.user.role.notificati on .description.errcode	tkt094	Die Anfrage zum Entfernen der Rolle {1} von Benutzer {0} wird bereits bearbeitet. Die Anfrage wurde von {3} an Universum {2} gesendet.
login.errors.invalidcredentials.errcode	tms001	Benutzer/Kennwort nicht gefunden.
login.errors.invalidcredentials.errcode	tms001	Versuchen Sie wicket/wicket als Benutzernamen und Kennwort
page.admin.failuremessage.errcode	tms002	{0} fehlgeschlagen.
error.validate.optionvalue.errcode	tms003	Der Wert {0} ist in {1} nicht zulässig.
error.validate.command.notfound.errcode	tms004	Befehls-ID {0} nicht gefunden.
error.validate.command.disabled.errcode	tms005	Befehls-ID {0} ist nicht aktiviert.
error.addattachment.noname.errcode	tms006	Anhang konnte nicht gespeichert werden, füllen Sie den Namen des Feldes aus.
error.filter.errcode	tms007	Der Filter '{0}' hat einen Syntaxfehler. {1}
error.filter.resultempty.errcode	tms008	Der Benutzer existiert nicht.
error.command.revokecmd.errcode	tms009	Ticket konnte nicht widerrufen werden {0}; Jobtickets {1} fehlen.
error.command.revokecmd.msg2.errcode	tms010	Ticket {0} mit den Jobtickets {1} konnte nicht widerrufen werden; {2} Aktivitätstickets befinden sich außerhalb der Ticketstruktur.
error.command.linkcommands.errcode	tms011	Befehle konnten nicht erstellt werden: {0}, {1}

Feld	Code	Beschreibung
error.command.startjobcommand.errcode	tms012	Der Job für das Ticket {0} konnte nicht gestartet werden; das Ticket hat bereits eine Referenz für den Job {1}
error.command.startjobcommand.checkjobticket exists.errcode	tms013	Aktivität [checkjobticketexists] in Job [{1}] des Tickets {0} konnte nicht übergeben werden; überprüfen Sie den TMS-Port im Workpoint-Webservice für den WFTMS.
error.workflow.connection.errcode	tms014	Es konnte keine Verbindung zur Workpoint-URL hergestellt werden:{0}, Info:{1}
error.service.createconsulttickets.errcode	tms015	Kein übergeordnetes Ticket!
error.service.createconsulttickets2.errcode	tms016	Suche nach Konsultierungsbenutzern fehlgeschlagen, {0}
error.service.createconsulttickets3.errcode	tms017	Konsultierungstickets konnten nicht erstellt werden. {0}
error.service.validatevalue.errcode	tms018	Das Feld {0} konnte nicht mit dem Wert {1} im Tickettyp {2} aktualisiert werden
error.command.saveticket.optimisticlockexceptio n .errcode	tms019	Das Ticket wurde von einem anderen Benutzer aktualisiert, öffnen Sie das Ticket erneut.
error.validate.valuelength.errcode	tms020	Validierung fehlgeschlagen für den Wert: {0} kann nicht länger als {1} sein
error.validate.date.errcode	tms021	Datum konnte nicht analysiert werden: {0}"
error.batchtask.errcode	tms022	[{6}] Batch-Aktionsname konnte nicht ausgeführt werden
error.batchtask.startjob.errcode	tms023	Aktion {0} des Jobs {2} fehlgeschlagen. Wiederholungsanzahl: {1}
error.update.ticket.errcode	tms024	Ticket kann nicht aktualisiert werden [id
error.campaignnamenotfound.errcode	tms025	Kampagne {0} nicht gefunden.
page.recordnotfound.message.errcode	tms026	{0} nicht in {1} gefunden

Feld	Code	Beschreibung
page.internalerror.info1.errcode	tms027	Ein Fehler ist aufgetreten Weitere Informationen finden sie in der Protokolldatei.
page.internalerror.info2.errcode	tms028	null
page.expirederror.info1.errcode	tms029	Ihre Sitzung ist abgelaufen, melden Sie sich erneut an.
page.expirederror.info2.errcode	tms030	null
error.workpoint.dbconnection.errcode	tms031	Verbindung zur Workpoint-Datenbank getrennt.
text.dialogs.runfailed.errcode	txd001	{0} konnte nicht ausgeführt werden. Details finden Sie in den Protokolldateien.
text.dialogs.runfailed.errcode	txs002	{0} konnte nicht ausgeführt werden. Details finden Sie in den Protokolldateien.
settings.strings.universe.masterequalmodel.errcode	ust001	Warnung!!! Master- und Modellkonfigurationen sind gleich.
settings.strings.universes.errors.missingname .errcode	ust002	Feld 'Name' fehlt.
settings.strings.universes.errors.missingdescription .errcode	ust003	Feld 'Beschreibung' fehlt.
settings.strings.universes.errors.namealreadyexist .errcode	ust004	doppelter Name, Name wird bereits verwendet.
settings.strings.universes.errors.missingmaster .errcode	ust005	Feld mit dem Namen der Masterkonfiguration fehlt.
settings.strings.universes.errors.missingmodel .errcode	ust006	Feld mit dem Namen der Modellkonfiguration fehlt.
settings.strings.universes.errors.missingauditsettingsfile.errcode	ust007	Audit-Einstellungsdatei {0} nicht gefunden.
settings.strings.universes.errors.masterisnotreadonly .errcode	ust008	die Masterkonfiguration ({0}) ist nicht schreibgeschützt.
settings.strings.universes.errors.masterhasparent .errcode	ust009	die Masterkonfiguration ({0}) hat eine übergeordnete Konfiguration.

Feld	Code	Beschreibung
settings.strings.universes.errors.masternotlogged .errcode	ust010	die Modellkonfiguration ({0}) wird nicht protokolliert.
settings.strings.universes.errors.modelisnotreado nly .errcode	ust011	die Modellkonfiguration ({0}) ist nicht schreibgeschützt.
settings.strings.universes.errors.modelhasparent. errcode	ust012	die Modellkonfiguration ({0}) hat eine übergeordnete Konfiguration.
settings.strings.universes.errors.modelnotlogged .errcode	ust013	die Modellkonfiguration ({0}) wird nicht protokolliert.
settings.strings.universes.errors.errorswasfound .errcode	ust014	Die folgenden Probleme wurden gefunden:
settings.strings.universes.errors.wouldliketoautof ix .errcode	ust015	möchten Sie diese automatisch beheben?
error.workpoint.dbconnection.errcode	wp001	Verbindung zur Workpoint-Datenbank getrennt.

Anhang A: CA RCM-Eigenschaften

Dieses Kapitel enthält folgende Themen:

tms.delegate.filter

Wird zur Filterung der Liste verwendet, die mögliche Benutzer zur Delegierung enthält. Es stehen drei Optionen zur Verfügung:

Beschreibung	Standarddelegierungsfilter
Eigenschaft	tms.delegate.filter
Beispiel	tms.delegate.filter=GFilter=(Organization=$$owner.Organization$$)
Beschreibung	Tickettypfilter
Eigenschaft	tms.delegate.filter.TicketType.SAGE.ChangeApprovalParentTicket
Beispiel	tms.delegate.filter.TicketType.SAGE.ChangeApprovalParentTicket=GFilter=(Organization=cookingdept)
Beschreibung	Ticketnamensfilter
Eigenschaft	tms.delegate.filter.LinkUser-Role
Beispiel	tms.delegate.filter.LinkUser-Role=GFilter=(Email=ssimhi@eurekify.com)

Die Eigenschaft "Name" (wenn definiert) steht über “Typ” und diese Eigenschaft wiederum über "Standarddelegierung".

tms.escalate.filter

Wird zur Filterung der Liste verwendet, die mögliche Benutzer zur Eskalierung enthält. Es stehen drei Optionen zur Verfügung:

Beschreibung	Standardeskalierungsfilter
Eigenschaft	tms.escalate.filter
Beispiel	tms.escalate.filter=GFilter=(Organization=$$owner.Organization$$)
Beschreibung	Tickettypfilter
Eigenschaft	tms.escalate filter.TicketType.SAGE.ChangeApprovalParentTicket
Beispiel	tms.escalate.filter.TicketType.SAGE.ChangeApprovalParentTicket=GFilter=(Organizatio n= cookingdept)
Beschreibung	Ticketnamensfilter
Eigenschaft	tms.escalate.filter.LinkUser-Role
Beispiel	tms.escalate.filter.LinkUser-Role=GFilter=(Email=ssimhi@eurekify.com)

tms.campaign.[campaign-type].reassign.filter

Wird zur Filterung der Liste verwendet, die mögliche Benutzer zur Neuzuweisung enthält. Es stehen drei Optionen zur Verfügung:

Beschreibung	Neuzuweisungsfilter
Eigenschaft	tms.campaign.[campaign-type].reassign.filter
Beispiel	tms.campaign.userCertification.reassign.filter=GFilter=(Organization= $$owner.Organization$$) tms.campaign.roleCertification.reassign.filter=GFilter=(Organization= $$owner.Organization$$) tms.campaign.resourceCertification.reassign.filter=GFilter=(Organization= $$owner.Organization$$)

Anhang B: Portalstruktur (XML)

Wenn Sie die CA RCM-Portal-Struktur ändern und zum Beispiel einen Abschnitt des Portals entfernen möchten, den Sie niemals verwenden, können Sie die "portal-structure.xml"-Datei nach Bedarf bearbeiten. Die "portal-structure.xml"-Datei befindet sich an den folgenden Speicherorten:

- JBoss: *Jboss_install_folder*/conf
- WebSphere: /eurekify.war/WEB-INF/classes/com/eurekify/web/portal/links

Anhang C: CA RCM-Datendateien

CA RCM verwendet drei separate aber zueinander verwandte Dateien in textbasiertem, durch Kommas getrenntem Format, um eine Konfiguration zu repräsentieren.

Die Benutzer- und Ressourcendatenbankdateien enthalten die Basisfunktionen von Benutzern und Ressourcen. Die Konfigurationsdatei enthält die dynamischen Teile einer Konfiguration, das heißt, die Rollen und Beziehungen/Verbindungen.

Dieses Kapitel enthält folgende Themen:

Beispiel: Benutzerdatenbankdatei

Dateinamen der Benutzerdatenbank enden mit dem Suffix ".udb". Jeder Benutzer wird in dieser Datei in einer Zeile dargestellt, wobei für die folgenden Felder (in dieser Reihenfolge) durch Kommas getrennte Werte zu finden sind:

- Personen-ID (Schlüssel)
- Benutzername
- Organisationsname
- Organisationstyp
- (Optional) Eine unbegrenzte Anzahl zusätzlicher Felder.

Obwohl die Angabe optional ist, erfordert CA RCM, dass Sie Felder für die folgenden Benutzerinformationen angeben, wenn Sie ein Universum angeben. Geben Sie diese Felder in den ".udb"-Dateien an, die die Grundlage für eine Konfigurationsdatei in einem Universum bilden.

- Anmelde-ID
- Benutzer-E-Mail
- Manager-ID

Beispiel: Benutzerdatenbankdatei

Die folgende Beispieldatei mit der Endung ".udb" enthält 3 Benutzerdatensätze.

```
PersonID,UserName,OrgName,OrgType,Country,Location,ManagerID,email,LoginID,
"52656727","Rodman Adam","System
Management","Corporate","US","Pennsylvania","54672910","52656727@company.com","IB
MR50\\Rodman Adam",
"54672910","Cooper Amos","IT
Security","Corporate","US","Pennsylvania","64646410","54672910@company.com","IBMR
50\\Cooper Amos",
"64646410","Herman Barbara","Operations","Corporate","US","New
Jersey","64646410","64646410@company.com","IBMR50\\Herman Barbara",
```

Ressourcendatenbankdatei

Dateinamen der Ressourcendatenbank enden mit dem Suffix ".rdb". Jede Ressource wird in dieser Datei in einer Zeile dargestellt, wobei für die folgenden Felder (in dieser Reihenfolge) durch Kommas getrennte Werte zu finden sind:

- Ressourcenname 1 (ResName1)
- Ressourcenname 2 (ResName1)
- Ressourcenname 3 (ResName1)
- (Optional) Eine unbegrenzte Anzahl zusätzlicher Felder.

Die Felder "ResName" weisen normalerweise zum Endpunkt oder der Anwendungsgruppe der Ressource zu.

Obwohl die Angabe optional ist, erfordert CA RCM, dass Sie Felder für die folgenden Ressourceninformationen angeben, wenn Sie ein Universum angeben. Geben Sie diese Felder in den ".rdb"-Dateien an, die die Grundlage für eine Konfigurationsdatei in einem Universum bilden.

- Anwendung
- Manager-ID

Beispiel: Ressourcendatenbankdatei

Die folgende Beispieldatei enthält 3 Ressourcendatensätze.

```
ResName1,ResName2,ResName3,Description,ManagerID-Owner,Location,
"SYS1","RACFPROD","RACF22","Production RACF","77292450","Irvine,CA",
"Domain Users","NT5AVE","WinNT","Active Directory ","91236370","Houson,TX",
"DEVELOP","RACFPROD","RACF22","Production RACF","77292450","Irvine,CA",
```

Konfigurationsdatei

Konfigurationsdateinamen haben die Endung ".cfg". Die Konfigurationsdatei bezieht sich auf eine Benutzerdatenbankdatei und eine Ressourcendatenbankdatei. Sie enthält Rollendefinitionen und verknüpft Benutzer, Rollen und Ressourcen.

Hinweis: Mehrere Konfigurationen können die gleichen Benutzer- und Ressourcendatenbankdateien gemeinsam nutzen.

Die Konfigurationsdatei enthält die folgenden Elemente:

- Der Kopfabschnitt listet den Eigentümer und den Änderungsverlauf der Datei auf. Die ersten zwei Zeilen in der Datei geben die Benutzer- und Ressourcendatenbankdateien an, auf die sich die Konfiguration bezieht. Diese Zeilen haben folgendes Format:

  ```
  UsersDB,udb_Pfadname
  ResDB,rdb_Pfadname
  ```

  Hinweis: *udb_Pfadname* ist der Pfadname der entsprechenden Benutzerdatenbankdatei und *rdb_Pfadname* ist der Pfadname der entsprechenden Ressourcendatenbankdatei.

- Angaben zur Benutzer-Entität geben eine Teilmenge von Benutzern aus der entsprechenden Benutzerdatenbankdatei an. Jede Zeile gibt einen einzelnen Benutzer mit dem folgenden Format an:

  ```
  User, udb_Datensatz, Personen-ID
  ```

  Hinweis: *udb_Datensatz*ist der Indexwert eines Datensatzes in der Benutzerdatenbankdatei. Der erste Benutzerdatensatz in der Datei ".udb" hat einen Indexwert von Null. *Person-ID* ist der Wert des Feldes "Personen-ID" im entsprechenden Benutzerdatensatz.

- Angaben zur Ressourcen-Entität geben eine Teilmenge von Ressourcen aus der entsprechenden Ressourcendatenbankdatei an. Jede Zeile gibt eine einzelne Ressource mit dem folgenden Format an:

  ```
  Res, rdb_Datensatz, ResName1, ResName2, ResName3
  ```

  Hinweis: *rdb_Datensatz* ist der Indexwert eines Datensatzes in der Ressourcendatenbankdatei. Der erste Benutzerdatensatz in der Datei ".rdb" hat einen Indexwert von Null. *ResName1*, *ResName2*, *ResName3* sind die Werte der entsprechenden obligatorischen Felder im entsprechenden Ressourcendatensatz.

- Angaben zu Rollen definieren eine Rolle in Bezug auf Benutzer, Ressourcen oder andere Rollen in der Konfiguration. Jede Angabe definiert eine einzelne Rolle in einer Zeile mit dem folgenden Format:

  ```
  Rolle,Rollen-
  ID,Rollenname,Rollenbeschreibung,Rollenorganisation,Rolleneigentümer
  ```

  Hinweis: *Rollen-ID* ist der numerische Bezeichner, den CA RCM einer Rolle zuweist, *Rollenname* ist der eindeutige Name der Rolle, *Rollenbeschreibung* ist eine Textbeschreibung der Rolle, *Rollenorganisation* ist die mit der Rolle verknüpfte Organisation und *Rolleneigentümer* ist der Benutzer, der die Rolle besitzt.

- Angaben für Links definieren Rolleninhalte und Benutzerberechtigungen als eine Reihe von Links zwischen den angegebenen Benutzer-, Rollen- und Ressourcen-Entitäten. Jede Zeile gibt einen einzelnen Link mit dem folgenden Format an:

  ```
  Linktyp,Entität1,Entität2
  ```

  Hinweis: *Linktyp* gibt den Typ der Verknüpfung an. *Entität1* und *Entität2* geben die verknüpften Entitäten an, unter Verwendung des Datensatzindexes eines Benutzers oder Ressourcenentität, oder der Rollen-ID einer Rollenentität.

  Die Zeichenkette für *Linktyp* kann die folgenden Werte haben:

  - User-Res: Link zwischen Benutzer und Ressource
  - User-Role: Link zwischen Benutzer und Rolle
  - Role-Res: Link zwischen Rolle und Ressource
  - Role-Role - Link zwischen Rolle und Rolle (Link zwischen übergeordneten und untergeordneten Elementen in der Rollenhierarchie)

  Entitäten müssen in Reihenfolge aufgelistet werden. Zum Beispiel ist in der Angabe "User-Res" die erste Entität ein Benutzerdatensatz und die zweite Entität ein Ressourcendatensatz. In einem Link zwischen zwei Rollen ist die erste Entität die Rollen-ID der übergeordneten Rolle und die zweite Entität die Rollen-ID der untergeordneten Rolle.

Beispiel: Konfigurationsdatei

Konfigurationsdateien sind normalerweise viel länger als dieses Beispiel. In diesem Beispiel hat Rolle 1001 nur eine Ressource, Rolle 1014 hat zwei Ressourcen, und Rolle 1015 enthält sowohl Rolle 1001 als auch Rolle 1014 als untergeordnete Elemente.

```
UsersDB,.\UsersDB.udb
ResDB,.\ResDB.rdb
CreateDate,03/09/2007 12:27
ModifyDate,03/09/2007 12:27
StatusDate,17/04/2007 15:36
Owner1,Ilan Sharoni
Organization1,Company
Owner2,
Organization2,
Operation1,
Operation2,
Operation3,
Status,
ParentConfigName,SQL://(local).sdb/ConfigWithRoles.cfg
User,0,"45489940"
User,1,"47868650"
User,2,"52656727"
Res,0,"APPLDEV","RACFTEST","RACF22"
Res,1,"BRLIMSYS","RACFPROD","RACF22"
Res,2,"DEVELOP","RACFPROD","RACF22"
Role,1001,"BASIC ROLE","Basic role - for all IT
users","Enterprise","82922230","Org Role","","45489940","Approved","09/05/2007
10:36","No Rule","Enterprise","Corporate",""
Role,1014,"Title - Product Manager","Characteristic Role (50%)","Title - Product
Manager","99883135","Org Role","","45489940","Approved","09/05/2007
10:36","Title=Product Manager;","Title","Corporate",""
Role,1015,"Title - Operator","Characteristic Role (50%)","Title -
Operator","45489940","Org Role","","45489940","Approved","09/05/2007
10:36","Title=Operator;","Title","Corporate",""
User-Res,0,2
User-Res,0,1
User-Role,1,1001
User-Role,2,1014
Role-Res,1001,0
Role-Res,1014,1
Role-Res,1014,2
Role-Role,1015,1014
Role-Role,1015,1001
```

Terminologieglossar

Auditkarte

Eine Datei mit der Endung .aud. Sie wird durch die DNA generiert. Sie enthält eine Liste an Verletzungen oder "Out-Of-Pattern"-Situationen. Jeder Eintrag ist eine Verletzung, die mit einer Entität oder einem Link verbunden ist. Eine Auditkarte kann im DNA-Modul bearbeitet werden, wenn Anweisungen dazu hinzugefügt werden, ob eine Verletzung repariert oder genehmigt werden soll. Weitere Informationen finden Sie im DNA-Benutzerhandbuch.

Connectors

Connectors verwenden die Konverter, um sowohl für Download- als auch Upload-Vorgänge auf den Produktionscomputer zuzugreifen. Es gibt separate Connectors für Import- und Exportprozeduren.

defaultSettings.xml

Eine XML-Datei mit Verbindungsdetails ist im CA RCM-Basisverzeichnis des Konverterunterverzeichnisses zu finden. Verwenden Sie zur Aktualisierung das CA RCM-DM-Modul

Direkter Link

Eine Verbindung ohne Zwischenschritte zwischen zwei Entitäten. Zum Beispiel: Link zwischen Benutzer und Ressource.

Dualer Link

In diesem Fall ist sowohl ein direkter als auch ein indirekter Link vorhanden. Zum Beispiel: Ein Benutzer ist direkt mit einer bestimmten Ressource verbunden, derselbe Benutzer ist jedoch auch mit einer Rolle verbunden, die mit derselben Ressource verlinkt ist.

Entität

Bezieht sich auf eine der folgenden Optionen:

- Benutzer
- Rolle
- Ressource

Genehmigte Auditkarte

Eine Auditkarte, bei der alle aufgelisteten Verletzungen genehmigt worden sind. Sie kann während eines Audits verwendet werden, um zu verhindern, dass bereits genehmigte Verletzungen erneut gemeldet werden.

Indirekter Link

Eine über einen Umweg bestehende Verbindung zwischen zwei Entitäten. Zum Beispiel: Ein Benutzer ist mit einer bestimmten Rolle verbunden und die Rolle ist mit einer bestimmten Ressource verbunden. Die Verbindung zwischen dem Benutzer und der Ressource ist ein indirekter Link. Hier einige weitere Beispiele:
Benutzer—Rolle—Ressource: Indirekter 'Benutzer-zu-Ressource'-Link
Benutzer—Rolle—Rolle: Indirekter 'Benutzer-zu-Rolle'-Link (Hierarchie)
Benutzer—Rolle—Rolle—Ressource: Indirekter 'Benutzer-zu-Ressource'-Link
Indirekte Links sind nicht für den Fall 'Benutzer zu Ressource zu Rolle' definiert, bei dem der Benutzer direkt mit einer Ressource und eine Rolle direkt mit derselben Ressource verbunden sind. In diesem Fall besteht zwischen dem Benutzer und besagter Rolle kein Link.

Konfiguration

Eine CA RCM-eigene Datenstruktur, die einen Snapshot mit Definitionen von Benutzern, Ressourcen und Rollen (falls verfügbar) enthält, sowie die relevanten Beziehungen (Privilegien) zwischen ihnen.

Link oder Entitätslink

Dies bezieht sich auf eine Verbindung zwischen zwei Entitäten. Die möglichen Links lauten:

- Benutzer-Rolle
- Benutzer-Ressource
- Rolle-Ressource
- Rolle-Rolle (Hierarchie)

Links können als direkte, duale oder indirekte Links kategorisiert werden.

Masterkonfiguration

Die originale Konfiguration, heruntergeladen vom Produktionscomputer. Die Masterkonfiguration präsentiert die tatsächlichen Definitionen.

Modelkonfiguration

Eine Kopie der Masterkonfiguration. Der Auditprozess wird an der Modellkonfiguration ausgeführt und der daraus resultierende, aktualisierte Konfigurationsdateiensatz wird durch das Eurekify-Sage-DNA-System mit den originalen Masterkonfigurations-Dateien verglichen. Die Unterschiede werden dann auf den Produktionscomputer hochgeladen.

RACI

Ein RACI-Diagramm, auch RACI-Matrix genannt, wird verwendet, um die Rollen und Zuständigkeiten verschiedener Teams oder Benutzer zu beschreiben. Es ist besonders nützlich, wenn es darum geht, Rollen und Zuständigkeiten in funktions-/abteilungsübergreifenden Projekten und Prozessen zu spezifizieren. Innerhalb des Eurekify-Portals ist dies die in diesem Handbuch erwähnte Quelle der Genehmiger. Sie sind in der 'Accountable'-Konfigurationsdatei aufgelistet. Das RACI-Diagramm teilt Aufgaben in vier teilnehmende Zuständigkeitstypen, die dann verschiedenen Rollen des Projekts oder Prozesses zugewiesen werden. Folgende Zuständigkeitstypen bilden das Acronym RACI:

Responsible (Verantwortlich)

Diejenigen, die arbeiten, um die Aufgabe zu erfüllen. Mehrere Ressourcen können 'responsible' (verantwortlich) sein.

Accountable

(Auch 'Approver' (Genehmiger)) Die eigentlich ausschlaggebende Ressource für die korrekte und sorgfältige Fertigstellung der Aufgabe. Für jede Aufgabe darf nur eine A-Ressource angegeben sein.

Consulted (konsultiert)

Diejenigen, deren Meinung erfragt wird. Zwei-Wege-Kommunikation.

Informed (Informiert)

Diejenigen, die kontinuierlich über den Verlauf informiert werden. Ein-Weg-Kommunikation.

Sehr oft ist die als "accountable" angegebene Rolle auch als "responsible" festgelegt. Abgesehen von dieser Ausnahme wird allgemein empfohlen, dass jede Rolle im Projekt oder Prozess für jede Aufgabe höchstens einen der teilnehmenden Rollentypen erhält. Auch wenn manche Unternehmen oder Organisationen beispielsweise doppelt teilnehmende Typen zulassen, bedeutet dies normalerweise, dass die Rollen noch nicht wirklich beschlossen sind, wodurch der Wert des RACI-Versuchs, jede Rolle auf eine Aufgabe zu spezifizieren, beeinträchtigt wird. Weitere Informationen zu RACI finden Sie unter http://www.pmforum.org/library/tips/pdf_files/RACI_R_Web3_1.pdf.

'Rolle-zu-Rolle'-Link

Dieser Linktyp stellt eine hierarchische Beziehung dar. Benutzer, die Mitglieder einer übergeordneten Rolle sind, sind automatisch Mitglieder der Unterrolle und verfügen daher über alle Unterrollen-Berechtigungen.

Ticket

Tickets sind Arbeitselemente, die in der Ticketwarteschlange angezeigt werden. Sie können Arbeits- oder Informationszwecken und/oder hierarchischen Zwecken dienen oder eine schlichte Benachrichtigung bezüglich eines Prozesses liefern.

Universum

Ein Begriff, mit dem ein einziges Master-Konfigurations/Modell-Konfigurations-Paar angegeben wird.

Untergeordnete Elemente

Tickettyp-spezifisch.
Die Anzahl der für ein Kampagnenticket aufgelisteten untergeordneten Elemente gibt die Anzahl der Genehmiger an, die der Kampagne zugewiesen sind.
Die Anzahl der für ein Genehmigerticket aufgelisteten untergeordneten Elemente entspricht der Anzahl der [Entitäten], die der jeweilige Genehmiger auditieren muss, wobei sich [Entitäten] auf den Kampagnentyp beziehen: Benutzer-, Rollen- oder Ressourcenzertifizierung.

Verletzungen

Eine Verletzung ist ein Verstoß der Richtlinien, Leitlinien, BPRs bzw. Regelungen im Hinblick auf die Unternehmenssicherheit. CA RCM identifiziert solche Verstöße und listet sie, wenn sie relevant sind, in Auditkarten auf. Bei der Verwendung des CA RCM-Portals werden Sie auf mit 'Verletzungen' betitelte Spalten stoßen, wo sie relevant sind. Die in solchen Spalten aufgelistete Zahl zeigt die Anzahl der Verletzungen an, die mit der jeweiligen Reihe der Tabelle assoziiert werden.

Workflow

Kampagnen und Genehmigungsvorgänge werden von einem Workflow gesteuert, einer Sammlung an Anweisungen, die die Anwendungslogik steuern. Der Workflow wird von Workpoint™ generiert, einem Entwurfs-Engine für den Workflow von Geschäftsprozessmanagement (BPM).

Zuordnung.xml

Eine sich im <Eurekify Basisverzeichnis>\<Konverterverzeichnis> befindende XML-Datei mit Zuordnungsdetails. Verwenden Sie zur Aktualisierung das Eurekify-DM-Modul.

Index